

## Spectralink VIEW Certified Configuration Guide

# Aruba Networks

Aruba Controllers (Series) 600, 3200, 3400, 3600, 6000, 7000, 7100, 7200

Aruba APs AP-60, AP-61, AP-65, AP-68, AP-70, AP-9x, AP-10x, AP-11x, AP-12x, AP-13x, AP-22x, AP-27x

## Copyright Notice

© 2005-2015 Spectralink Corporation All rights reserved. Spectralink™, the Spectralink logo and the names and marks associated with Spectralink's products are trademarks and/or service marks of Spectralink Corporation and are common law marks in the United States and various other countries. All other trademarks are property of their respective owners. No portion hereof may be reproduced or transmitted in any form or by any means, for any purpose other than the recipient's personal use, without the express written permission of Spectralink.

All rights reserved under the International and pan-American Copyright Conventions. No part of this manual, or the software described herein, may be reproduced or transmitted in any form or by any means, or translated into another language or format, in whole or in part, without the express written permission of Spectralink Corporation.

Do not remove (or allow any third party to remove) any product identification, copyright or other notices.

## Notice

Spectralink Corporation has prepared this document for use by Spectralink personnel and customers. The drawings and specifications contained herein are the property of Spectralink and shall be neither reproduced in whole or in part without the prior written approval of Spectralink, nor be implied to grant any license to make, use, or sell equipment manufactured in accordance herewith.

Spectralink reserves the right to make changes in specifications and other information contained in this document without prior notice, and the reader should in all cases consult Spectralink to determine whether any such changes have been made.

NO REPRESENTATION OR OTHER AFFIRMATION OF FACT CONTAINED IN THIS DOCUMENT INCLUDING BUT NOT LIMITED TO STATEMENTS REGARDING CAPACITY, RESPONSE-TIME PERFORMANCE, SUITABILITY FOR USE, OR PERFORMANCE OF PRODUCTS DESCRIBED HEREIN SHALL BE DEEMED TO BE A WARRANTY BY SPECTRALINK FOR ANY PURPOSE, OR GIVE RISE TO ANY LIABILITY OF SPECTRALINK WHATSOEVER.

## Contact Information

### US Location

800-775-5330

Spectralink Corporation  
2560 55th Street  
Boulder, CO 80301

[info@spectralink.com](mailto:info@spectralink.com)

### European Location

+45 7560 2850

Spectralink Europe ApS  
Langmarksvej 34  
8700 Horsens, Denmark

[infodk@spectralink.com](mailto:infodk@spectralink.com)

# Contents

<b>Introduction.....</b>	<b>6</b>
<b>Certified Product Summary.....</b>	<b>6</b>
<b>Known Limitations.....</b>	<b>7</b>
<b>Spectralink References .....</b>	<b>9</b>
<i>Support documents .....</i>	<i>9</i>
<i>White Papers.....</i>	<i>10</i>
<b>Product Support .....</b>	<b>10</b>
 <b>Section 1: Configuration for Wi-Fi Standard QoS .....</b>	<b>11</b>
<b>Introduction.....</b>	<b>11</b>
<b>Command, Comment, and Screen Text Key .....</b>	<b>11</b>
<b>Network Topology.....</b>	<b>12</b>
<b>Connecting to the Mobility Controller .....</b>	<b>13</b>
<i>Via console.....</i>	<i>13</i>
<i>Via the Command Line Interface (CLI) .....</i>	<i>13</i>
<i>Via the Web interface (WebUI).....</i>	<i>13</i>
<b>Initializing the Controller .....</b>	<b>15</b>
<b>Licensing the Controller .....</b>	<b>17</b>
<b>Logical and Physical Interfaces.....</b>	<b>19</b>
<i>Using CLI .....</i>	<i>19</i>
<i>On the WebUI .....</i>	<i>20</i>
<b>Creating Firewall Roles and Policies.....</b>	<b>23</b>
<b>Creating a Syslog Policy .....</b>	<b>24</b>
<i>On CLI.....</i>	<i>24</i>
<i>On WebUI .....</i>	<i>24</i>
<b>Creating User-Role and Assigning Firewall Rules to the Role .....</b>	<b>26</b>
<i>On CLI.....</i>	<i>26</i>
<i>On WebUI .....</i>	<i>26</i>
<b>Creating a User-Role Derivation Rule.....</b>	<b>28</b>
<i>On CLI.....</i>	<i>28</i>
<i>On WebUI .....</i>	<i>28</i>
<b>Configuration Steps for None, WEP, WPA-PSK or WPA2-PSK Security.....</b>	<b>30</b>
<i>Creating an Authentication Profile for controller-based authentication .....</i>	<i>30</i>
<i>Use the next four statements if using an external Radius server: .....</i>	<i>30</i>
<b>Configuration Steps for WPA2-Enterprise Security .....</b>	<b>34</b>
<i>Defining an 802.1X authentication server .....</i>	<i>34</i>
<b>Create a Server Group and Add the RADIUS Server .....</b>	<b>36</b>
<i>Using CLI .....</i>	<i>36</i>
<i>Using WebUI.....</i>	<i>36</i>

<b>Creating an 802.1X Authentication Profile .....</b>	<b>37</b>
<i>Using CLI .....</i>	<i>37</i>
<i>Using WebUI .....</i>	<i>37</i>
<b>Creating an Authentication Profile .....</b>	<b>38</b>
<i>Using CLI .....</i>	<i>38</i>
<i>Using WebUI .....</i>	<i>38</i>
<b>Wireless LAN Configuration .....</b>	<b>40</b>
<i>On CLI .....</i>	<i>40</i>
<i>On WebUI .....</i>	<i>50</i>

## **Section 2: Configuration for SVP Operation with Spectralink 8020/8030 Handsets ..... 73**

<b>Introduction.....</b>	<b>73</b>
<b>Command, Comment, and Screen Text Key .....</b>	<b>73</b>
<b>Connecting to the Mobility Controller .....</b>	<b>74</b>
<i>Via console.....</i>	<i>74</i>
<i>Via the CLI .....</i>	<i>74</i>
<i>Via the Web interface (WebUI).....</i>	<i>74</i>
<b>Initializing the Controller .....</b>	<b>76</b>
<b>Licensing the Controller .....</b>	<b>78</b>
<b>Logical and Physical Interfaces.....</b>	<b>80</b>
<i>Using CLI .....</i>	<i>80</i>
<i>On the WebUI .....</i>	<i>80</i>
<b>Creating Firewall Roles and Policies.....</b>	<b>84</b>
<b>Creating a Syslog Policy .....</b>	<b>85</b>
<i>On CLI.....</i>	<i>85</i>
<i>On WebUI .....</i>	<i>85</i>
<b>Creating User-Role and Assigning Firewall Rules to the Role .....</b>	<b>87</b>
<i>On CLI.....</i>	<i>87</i>
<i>On WebUI .....</i>	<i>87</i>
<b>Creating a User-Role Derivation Rule.....</b>	<b>89</b>
<i>On CLI.....</i>	<i>89</i>
<i>On WebUI .....</i>	<i>89</i>
<b>Configuration Steps for None, WEP, WPA-PSK or WPA2-PSK Security.....</b>	<b>91</b>
<i>Creating an Authentication Profile for controller-based authentication .....</i>	<i>91</i>
<b>Configuration Steps for WPA2-Enterprise Security .....</b>	<b>95</b>
<i>Defining an 802.1X authentication server .....</i>	<i>95</i>
<b>Create a Server Group and Add the RADIUS Server .....</b>	<b>97</b>
<i>Using CLI .....</i>	<i>97</i>
<i>Using WebUI .....</i>	<i>97</i>
<b>Creating an 802.1X Authentication Profile .....</b>	<b>98</b>
<i>Using CLI .....</i>	<i>98</i>
<i>Using WebUI.....</i>	<i>98</i>

**Creating an Authentication Profile .....100**  
    *Using CLI ..... 100*  
    *Using WebUI ..... 100*  
**Wireless LAN Configuration .....102**  
    *On CLI..... 102*  
    *On WebUI ..... 107*

# Introduction

Spectralink's Voice Interoperability for Enterprise Wireless (VIEW) Certification Program is designed to ensure interoperability and high performance between Spectralink 84-Series, 87-Series, and 8020/8030 Wireless Telephones and WLAN infrastructure products.

The products listed below have been tested in Spectralink's lab and have passed VIEW Certification.

## Certified Product Summary

Manufacturer:	Aruba Networks: <a href="http://www.arubanetworks.com">www.arubanetworks.com</a>			
Certified products:	Controllers (Series): Aruba 600, 3200, 3400, 3600, 6000, 7000, 7100, 7200 Access Points: Aruba AP-60, 61, 65, 68, 70, 9x, 10x, 11x, 12x, 13x, 22x, 27x			
AP Radio(s):	2.4 GHz (802.11b/g/n), 5 GHz (802.11a/n)			
Security :	None, WEP, WPA-PSK, WPA2-PSK, WPA2-Enterprise (EAP-FAST and PEAPv0/MSCHAPv2)			
QoS:	Wi-Fi Standard for Spectralink 84-Series, 87-Series and 8020/8030 SVP for Spectralink 8020/8030			
AP/controller software version approved:	6.3.1.9 for 60, 61, 65, 68, 70, 9x, 105, 11x, 12x, 13x 6.4.2.3 for 22x, 27x (other APs testing not complete)			
Network topology	Switched Ethernet (recommended)			
<i>Handset* models tested:</i>	<i>Spectralink 8741/8753 Wireless Telephone (PIVOT)</i>			
AP radio mode:	802.11b	802.11b/g	802.11b/g/n	802.11a, a/n & a/n/ac
Meets VIEW minimum call capacity per AP:**	8	8	8	10

<i>Handset* models tested:</i>	<i>Spectralink 8440/8441/8450/8452/8453 Wireless Telephone</i>			
AP radio mode:	802.11b	802.11b/g	802.11b/g/n	802.11a, a/n, a/n/ac
Meets VIEW minimum call capacity per AP:**	8	8	8	10

<i>Handset models tested:</i>	<i>Spectralink 8020/8030 Wireless Telephone*</i>	
Handset radio mode:	802.11b/g mixed	802.11a
Meets VIEW minimum call capacity per AP:**	8 (SVP) 6 (Wi-Fi Standard QoS)***	12 (SVP) 8 (Wi-Fi Standard QoS)***

\*Spectralink handset models and their OEM derivatives are verified compatible with the WLAN hardware and software identified in the table. Throughout the remainder of this document they will be referred to collectively as “Spectralink wireless telephones”, “phones” or “handsets”. The 8440, 8441 (8440 with personal alarm hardware), 8450 (with 1D bar code reader), 8452 (with 1D and 2D bar code reader), and 8453 (8452 with personal alarm hardware) handsets will be referred to collectively as the 84-Series handsets. The 8741 and 8753 (with 2D bar code reader) will be referred to collectively as the 87-Series handsets.

\*\* Maximum calls tested per the VIEW Certification Test Plan. The certified product may actually support a higher number of maximum calls.

\*\*\* WPA2-Enterprise and Wi-Fi Standard QoS are not available for Spectralink 8020/8030 handsets connecting to traditional PBXs.

## Known Limitations

The following limitations were discovered during VIEW testing of this product

- 1Mb/s and 2Mb/s data rates must be disabled to meet maximum call capacity.
- “Legacy Station Workaround” must be enabled on the radio of an Aruba 11n/11ac AP to which the Spectralink wireless phone is connected.
- All handsets operating on a given AP radio must have the same QoS setting. The APs must be configured to enable the corresponding features to support the handset QoS setting.
- Heavy multicast, broadcast or push-to-talk (PTT) traffic may impair voice quality.
- Voice and data must be separated onto separate service set identifiers (SSIDs) to obtain the best voice performance.

- WPA2-Enterprise and Wi-Fi Standard QoS are not available for Spectralink 8020/8030 handsets connecting to traditional PBXs.
- Paired-channel deployment is not recommended on the 2.4 GHz radio by Aruba.
- The dynamic ARM and Client Match features, if enabled, may cause audio dropouts on the Spectralink handsets. The White Paper: *Best Practices Guide to Deploying Spectralink 84-Series Handsets* has more information about cell design. If ARM is on, it is recommended to check the VOIP Aware and Client Aware options. The use of VOIP Aware and Client Aware options was not tested by Spectralink during VIEW testing.
- 802.11r is not implemented on the Spectralink products
- The 87-Series handsets (PIVOT) have not yet implemented admission control using TSPECs. Admission control must be disabled on network where the 87-Series handsets are present.
- A-MPDU aggregation (an 802.11n feature) should be disabled in SSIDs used by the handsets. The handsets do not support this feature and there is an incompatibility in the Aruba implementation which causes poor handset performance.



## Spectralink References

All Spectralink documents are available at <http://support.spectralink.com>.

The screenshot shows the Spectralink Support website. At the top, there is a navigation bar with links for Partner Access, Spectralink.com, Contact Support, and a search bar. Below this is the Spectralink logo with the tagline 'solving every day' and the word 'support'. To the right of the logo are links for PRODUCT RESOURCES, RMAs, SERVICE REQUESTS, and CUSTOMER MANAGEMENT. The main heading is 'Welcome to Spectralink Support' with a subtext 'Find resources for your product, or log in for more support options.' Below this is a section titled 'PRODUCT RESOURCES' which contains a search area with dropdowns for 'Product Category' (set to 'Wi-Fi') and 'Product Type' (set to '- Any -'), and a 'FIND' button. To the right of the search area are links for 'All Documents & Downloads', 'Feature Requests', 'Product Alerts', 'Service Policies', 'FAQs', and 'Contact Support'. Below the search area are two sections: 'RMAs AND SERVICE REQUESTS' and 'CUSTOMER MANAGEMENT', each with a lock icon. The 'RMAs AND SERVICE REQUESTS' section contains links for 'RMA Status', 'My Service Requests', 'RMA Forms', 'My Company's Service Requests', 'RMA Requests', 'Repair Pricing', and 'My Company's RMAs'. The 'CUSTOMER MANAGEMENT' section contains links for 'Warranty and Entitlement Lookup', 'My Company's Entitlements', and 'Batch Warranty and Entitlement Lookup'. At the bottom, there is a copyright notice: '© 2013 Spectralink Corporation, All rights reserved. Terms and Conditions | Product Warranty'.

### To go to a specific product page

Select the Product Category and Product Type from the dropdown lists and then select the product from the next page. All resources for that particular product are displayed by default under the All tab. Documents, downloads and other resources are sorted by the date they were created so the most recently created resource is at the top of the list. You can further sort the list by the tabs across the top of the list to find exactly what you are looking for. Click the title to open the link.

### Support documents

*Spectralink 87-Series Wireless Telephone Administration Guide* The Admin Guide provides detailed information about every setting and option available to the administrator on both the CMS and handset menus. Time-saving shortcuts, troubleshooting tips and other important maintenance instructions are also found in this document.

*Spectralink 87-Series Wireless Telephone Deployment Guide* The Deployment Guide provides sequential information for provisioning and deploying the handsets. It covers deployment using the SLIC tool and CMS as well as manual deployment.

The *Spectralink 84-Series Wireless Telephone Administration Guide* provides a comprehensive list of every parameter available on Spectralink 84-Series Wireless Telephones.

The *Spectralink 84-Series Deployment Guide* is your essential reference for provisioning and deploying Spectralink 84-Series handsets in any environment.

The *Web Configuration Utility User Guide* explains how to use a web browser to configure the Spectralink 84-Series handsets on a per handset basis.

The *Spectralink 8020/8030 Wireless Telephone Handset Administration Tool* document explains how to use a software interface to configure the handsets.

## White Papers

Spectralink White Papers are available at <http://www.spectralink.com/resources/white-papers>.

For the Spectralink 84-Series Wireless Telephones, please refer to *Best Practices Guide for Deploying Spectralink 84-Series Handsets* for detailed information on wireless LAN layout, network infrastructure, QoS, security and subnets.

For the Spectralink 8020/8030 Wireless Telephones, please refer to *Best Practices Guide for Deploying Spectralink 80-Series Handsets*. This white paper covers the security, coverage, capacity and QoS considerations necessary for ensuring excellent voice quality with enterprise Wi-Fi networks.

For additional details on RF deployment please see the *Deploying Enterprise-Grade Wi-Fi Telephony*.

These White Papers identify issues and solutions based on Spectralink's extensive experience in enterprise-class Wi-Fi telephony. It provides recommendations for ensuring that a network environment is adequately optimized for use with Spectralink Wireless Telephones.

## Product Support



### **Note: RADIUS server configuration**

This document does not cover the steps involved to configure a RADIUS server required for using WPA2-Enterprise security types.

If you encounter difficulties or have questions regarding the configuration process, please contact Aruba customer service at: <http://www.arubanetworks.com/support.php> or Spectralink at [support.spectralink.com](http://support.spectralink.com).

# Section 1: Configuration for Wi-Fi Standard QoS

## Introduction

Spectralink 8020/8030 phones can be configured with Wi-Fi Standard QoS from the WLAN Settings menu using the Custom selection.

Spectralink 87-Series and 84-Series handsets only support Wi-Fi Standard QoS.

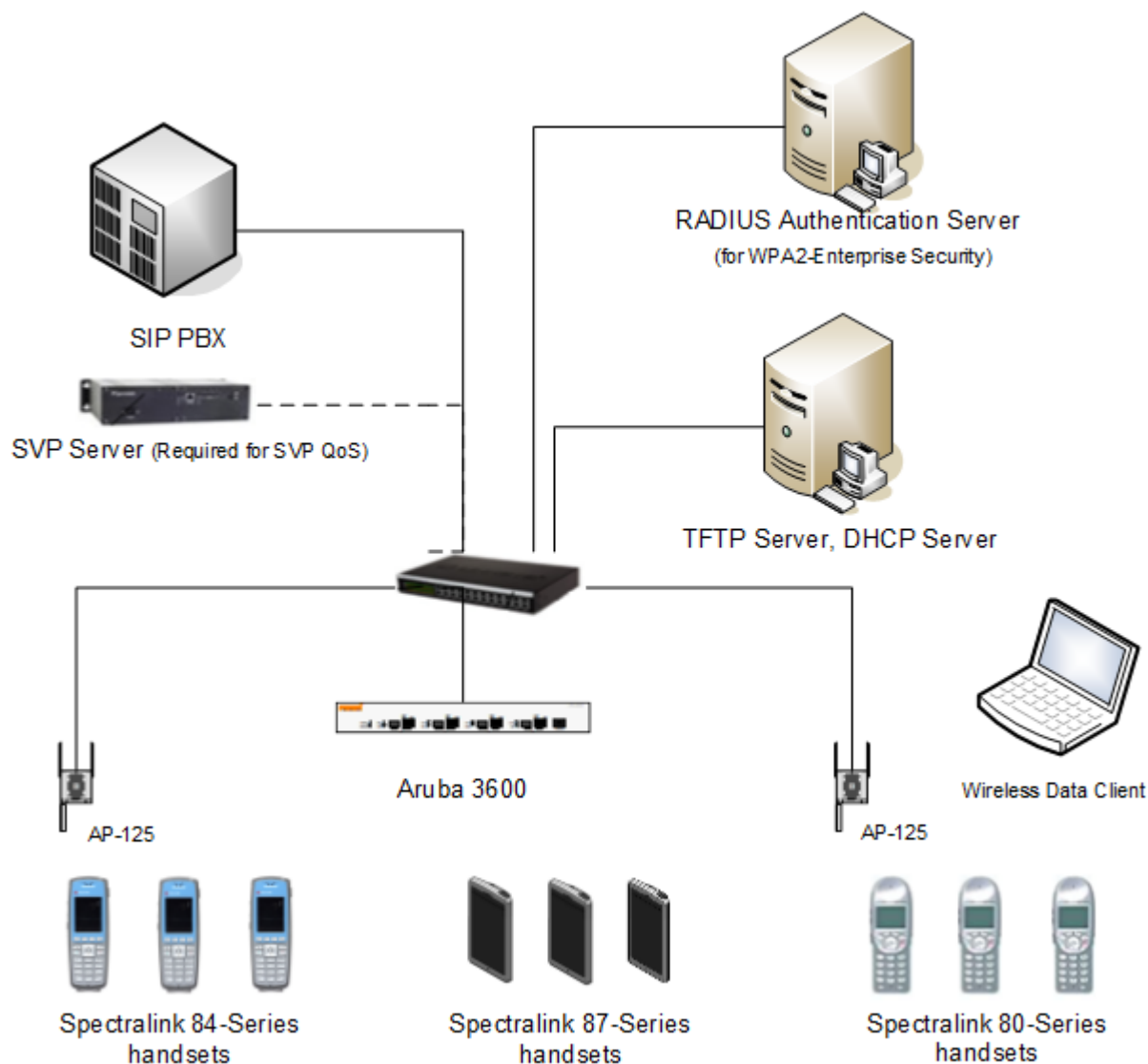
## Command, Comment, and Screen Text Key

In the sections below you will find commands, comments, prompts, system responses, or other screen-displayed information involved in the configuration process. This key explains the text styles and symbols used to denote them.

<b><i>Text Style</i></b>	<b><i>Denotes:</i></b>
<b>xxxxxxx</b>	Typed command
<b>&lt;xxxxxxx&gt;</b>	Encryption key, domain name or other information specific to your system that needs to be entered
<b>(xxxxxxx)</b>	Comment about a command or set of commands
<b>xxxxxxx</b>	Prompt, system response or other displayed information

## Network Topology

The following configuration was tested during VIEW Certification.



### Note: Example configuration shown

This is a modified diagram and not all components are shown for every system type.

## Connecting to the Mobility Controller

### Via console

Using a standard RS-232 cable, connect the Aruba mobility controller to the serial port of a terminal or PC.

Run a terminal emulation program (such as HyperTerminal™) or use a VT-100 terminal with the following configuration:

Bits per second:	9600
Data bits:	8
Parity:	None
Stop bits:	1
Flow control:	None

Use this mode of connection during the initialization phase of the controller to configure login credentials.

- 1 Press Enter to display the Aruba mobility controller login screen.
- 2 Enter the default login: **admin** and the default password: **admin**. These are case sensitive.
- 3 Enter **enable** and the default password: **enable** to get into the command mode.

### Via the Command Line Interface (CLI)

By default, only SSH (Secure Shell) access to the switch (mobility controller) is permitted.

- 1 From a management system that has network connectivity to the switch, connect to the switch using SSH

```
ssh admin@<switch IP address>
```

- 2 Enter the admin password at the password prompt.

```
Type enable at the > prompt to enter the enable mode.
```

- 3 Type the enable password when prompted for a password.

### Via the Web interface (WebUI)

Once the connectivity to the switch is verified, open a Web browser and enter the switch's IP address in the navigator bar.

The switch can be accessed using http at

**http://<switch IP Address>**

or https at

**https://<switch IP Address>:4343.**

The user is prompted with the username and password configured (in the example above, the username/password configured is **admin/admin**). On successful login the following **Monitoring** screen is displayed:

The screenshot displays the Aruba Mobility Controller interface. The top navigation bar includes tabs for Dashboard, Monitoring (selected), Configuration, Diagnostics, Maintenance, and Plan. The left sidebar lists various network categories: NETWORK (with a sub-menu for Network Summary), CONTROLLER, WLAN, VOICE, and DEBUG. The main content area shows the 'Network Summary' page, which includes a table titled 'WLAN Network Status'.

	Total Up	Total Down	IPSEC Up	IPSEC Down
WLAN Controllers	1	0		
Access Points	2	1	0	0
Mesh Portals	0	0		
Mesh Points	0	0		
Air Monitors	0	0	0	0
Wired Access Points	0	0	0	0
Unprovisioned Access Points	0			
Duplicate AP Name	0			

## Initializing the Controller

When powered up, the controller will present the following screen on the serial console. Please fill in basic network details when prompted. The following is a sample of the information presenting which may vary depending on the controller model and software version:

```
<<<<< Welcome to Aruba Networks - Aruba A651 >>>>>

Performing CompactFlash fast test... Checking for file system...
Passed.
Reboot Cause: User reboot.
Restoring the database...done.
Generating SSH Keys.....done.
Reading configuration from factory-default.cfg

***** Welcome to the Aruba651 setup dialog *****
This dialog will help you to set the basic configuration for the switch.
These settings, except for the Country Code, can later be changed from the
Command Line Interface or Graphical User Interface.

Commands: <Enter> Submit input or use [default value], <ctrl-I> Help
<ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end
<ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line
<ctrl-P> Previous question <ctrl-X> Restart beginning

Enter System name [Aruba651]
Enter VLAN 1 interface IP address [172.16.0.254]: <Controller IP>
Enter VLAN 1 interface subnet mask [255.255.255.0]: <Subnet Mask>
Enter IP Default gateway [none]: <Default GW IP address>
Enter Switch Role, (master|local) [master]
This controller is restricted to Country code US for United States, please
confirm (yes|no)? : yes
Enter Time Zone [PST-8:0]
Enter Time in GMT [15:39:55]
Enter Date (MM/DD/YYYY) [4/21/2009]
Enter Password for admin login (up to 32 chars): *****
Re-type Password for admin login: *****
```

```
Enter Password for enable mode (up to 15 chars): *****  
Re-type Password for enable mode: *****  
Do you wish to shutdown all the ports (yes|no)? [no]: no
```

Current choices are

```
System name: Aruba651  
VLAN 1 interface IP address: <IP Address>  
VLAN 1 interface subnet mask: <Subnet Mask>  
IP Default gateway: <Default Gateway>  
Switch Role: master  
Time Zone: PST-8:0  
Ports shutdown: no
```

```
If you accept the changes the switch will restart!  
Type <ctrl-P> to go back and change answer for any question  
Do you wish to accept the changes (yes|no): yes  
Creating configuration... Done.
```

System will now restart!



## *Licensing the Controller*

A license for the Next Generation Policy Enforcement Firewall Module must be installed for the firewall features and Spectralink voice prioritization to work. Please contact your local Aruba representative. License Management can be performed using the License Wizard of the WebUI.

You will need

- The Serial Number of the Mobility Controller.
- The License Certificate Number of the service to be activated (Please contact your local Aruba team).

Obtain the license Key from: <https://licensing.arubanetworks.com>

### **On the WebUI**

- 1** Click the **Configuration** tab.
- 2** On the tabs list, click **Licenses**.
- 3** Click **Add** by **Add New License Key** (scroll down to see option).
- 4** Enter the license Key in the space provided and click **OK**.
- 5** Repeat 3 and 4 for all the licenses desired.
- 6** Click **Save Configuration**.
- 7** Verify that the licenses show up on the table in the same screen.
- 8** Centralized Licensing and a license server may also be used. See the Aruba User's Guide for details.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
AP  
Controller  
Campus WLAN  
Remote AP  
AirWave  
NETWORK  
VLANs  
Ports  
Cellular Profile  
IP  
SECURITY  
Authentication  
Access Control  
WIRELESS  
AP Configuration  
AP Installation  
MANAGEMENT  
General  
Administration  
Certificates  
SNMP  
Logging  
Clock  
Guest Provisioning  
Captive Portal  
SMTP  
Bandwidth Calculator  
Threshold  
ADVANCED SERVICES  
Redundancy  
AirGroup  
IP Mobility  
Stateful Firewall  
External Services  
VPN Services  
Wired Access  
All Profiles

**Network > Controller > License Management**

System Settings Control Plane Security Cluster Settings **Licenses** Centralized Licenses Sync whitelist service

### License Information

Service Status and Current Limits		To obtain license keys via the web:
Access Points	32	<b>Licensing Web Site:</b> <a href="https://licensing.arubanetworks.com">https://licensing.arubanetworks.com</a> <b>You will need the following:</b> <ul style="list-style-type: none"> <li>The serial number of the switch or supervisory module</li> <li>The license certificate number of the service you wish to activate</li> </ul>
Remote Access Points	32	
Outdoor Mesh Access Points	512	<ul style="list-style-type: none"> <li>The serial number to use for this switch is: AC0002304</li> </ul>
RF Protect	0	
Voice Service Module	Unlimited	
VPN Server Module	8192	
xSec Module	0	
Indoor Mesh Access Points	512	
Next Generation Policy Enforcement Firewall Module	32	
Advanced Cryptography	0	
Service provider AP	0	
RF Protect	DISABLED	
Policy Enforcement Firewall	ENABLED	
Remote APs	ENABLED	
External Services Interface	ENABLED	
Client Integrity Module	ENABLED	
VPN Server	ENABLED	
xSec Module	DISABLED	
MMC AP	DISABLED	
Netgear AP	DISABLED	
Voice Services Module	ENABLED	
Mesh Point APs	ENABLED	
AP Developers Module	DISABLED	
Internal Test Functions	DISABLED	
Public Access	DISABLED	
Policy Enforcement Firewall for VPN users	DISABLED	
Advanced Cryptography	DISABLED	
Service Provider Access Point	DISABLED	
Maritime Regulatory Domain	DISABLED	

AP Licenses		User License Usage	
AP Licenses	32	License Limit	8192
PEF Licenses	32	License Usage	0
Overall AP License Limit	32	License Available	8192
		License Exceeded	0

AP Usage	
Active CAPs	1
Standby CAPs	0
RAPs	0
Remote-node APs	0
Tunneled nodes	0
Total APs	1

Remaining AP Capacity	
CAPs	31
RAPs	31

License Exceeded	
License Exceeded	0

xSec License Usage	
License Limit	0
License Usage	0
License Exceeded	0
xSec users	0
xSec tunnel	0

### License Table

Key	Installed	Expires	Flags	Service Type	Actions
rAj0GBvJ-NAY0Fhr8-4xd1V5ky-N9OXVb2w-40JQ6BPN-U84	2009-03-13 12:10:07	Never	E	Access Points: 32	Delete
Qs6QncVT-QTaRc9iS-At7hvQNm-ThjHKmjD-lWmTSEly-VsY	2011-08-03 06:54:54	Never	E	Next Generation Policy Enforcement Firewall Module: 32	Delete

Flags: A - auto-generated; E - enabled; R - reboot required to activate

Add New License Key

Add

Save Report Export Database Import Database

## Logical and Physical Interfaces

This section defines the Layer 2/3 framework that connects the Spectralink phones with the WLAN Mobility Controller (MC) and the Access Points. *The requirement is that the phones and Spectralink infrastructure be connected over Layer-2 and have the L2 subnet span across L3 switching/routing fabric.*

The steps involved are

- 1 Define a VLAN for voice on the WLAN.
- 2 Define the IP parameters for the VLAN.
- 3 Enable IGMP for use in the Push-to-talk function in the handsets.
- 4 Turn on the use of proxy ARP.
- 5 Define the DHCP server for the phones to get their IP addresses.
- 6 Define the physical port assignment on the MC. Most deployments have the MC uplinked to a Layer-3 switch which performs routing functions.

These parameters can be easily defined using the Controller Wizard on the WebUI.

### Using CLI

#### IP Interfaces, VLAN configuration

```
(Aruba651) #configure terminal
(Aruba651) (config) #vlan <vlan ID>
(Aruba651) (config) #interface <vlan ID>
(Aruba651) (config-subif) #ip igmp proxy <port(s) in use for PTT>
(Aruba651) (config-subif) #ip local-proxy-arp
(Aruba651) (config-subif) #ip helper-address <DHCP server / helper for the VLAN>
(Aruba651) (config-subif) #write m
(Aruba651) (config-subif) #end
```

#### Physical Port Assignment

The uplink is configured as follows

```
(Aruba651) (config) #interface gigabitethernet <slot/port>
(Aruba651) (config-if) #trusted
(Aruba651) (config-if) #no shutdown
(Aruba651) (config-if) #switchport mode trunk
(Aruba651) (config-if) #switchport trunk allowed vlan <VLAN IDs>
(Aruba651) (config-if) #write memory
```

## On the WebUI

- 1 Click the **Configuration** tab.
- 2 On the left pane, click **Controller** under **WIZARDS**.
- 3 The **Basic Info** and **Licenses** fields should be auto-filled from the previous steps. Click **Next** on both to arrive at the **VLANs** and **IP Interfaces** page.
- 4 Highlight the default VLAN line and click on it. (Other VLAN's may be entered here: see Aruba documentation for details.)
- 5 Enter details for the VLAN on which the phones are desired – VLAN ID, VLAN-Name.
  - a Click the drop-down to enter an IP address for the VLAN interface on the controller and the subnet mask. (Please bear in mind that L2 connectivity is required for the phones to reach the voice server and gateway).
  - b Click to choose the ports assigned to the VLAN (default is all available ports).
  - c Specify details on how the phones are expected to get their IP addresses. This drop-down offers the option of static IP assignment (**None**), DHCP using the in-built DHCP server (**Act as server**) and DHCP using an external DHCP server (**Relay to external**).

Named VLANs		All VLAN IDs on This Controller				
All		ID	IP Address/Netmask	Enable NAT	Port Members	DHCP Settings
		1	172.29.109.108/255.255.255.12	<input type="checkbox"/>	1/0,1/1,1/2,1/3	<input checked="" type="radio"/> None <input type="radio"/> Relay to external <input type="radio"/> Act as server

- 6 Click **Save Configuration**

Dashboard | Monitoring | **Configuration** | Diagnostics | Maintenance | Save Configuration

**Configure Controller**

Workflow | Help

- Basic Info  
Name: Aruba3600
- Licenses  
License Installed: 2
- VLANs and IP Interfaces**
- Connectivity
- Uplink
- Ports
- Finish

### Configure VLANs and IP Interfaces for Aruba3600

Configure VLANs for this controller. [More...](#)

Named VLANs		All VLAN IDs on This Controller				
	All	ID	IP Address/Netmask	Enable NAT	Port Members	DHCP Settings
		1	172.29.109.108/255.255.255.128	--	all	None

New Delete Add Delete

Back Next Cancel

- 7 Click **Next** to proceed to Connectivity assignment.
  - a Enter the IP address for the Default Gateway or pick Dynamic if the default gateway will be provided by DHCP, DNS, or router infrastructure.
  - b Click **Next**.
- 8 On **Ports**, enter the following
  - a By default, all ports are on VLAN 1. To change port configuration, click the corresponding row.
  - b If the controller has a single uplink to the wired network, check the **Trunk Mode** box for the port and include the VLANs to be trunked on that port.
  - c If the controller has only one uplink, STP should be disabled.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

**Configure Controller**

Workflow Help

- Basic Info  
Name: Aruba3600
- Licenses  
License Installed: 2
- VLANs and IP Interfaces  
VLAN Names: 0
- Connectivity  
Default Gateway: 172.29.109.1
- Uplink  
Uplink Ports:  
Uplink firewall: Disabled
- Ports**
- Finish

### Configure Ports for Aruba3600

Settings for all ports are shown in the table below. Select any row to edit it. [More...](#)

Fast Ethernet						
Port	Enabled	Trusted	Speed/Duplex	Native VLAN	Trunk Mode	VLANs for Trunk Mode

Gigabit Ethernet (edited)							Reset
Port	Enabled	Trusted	Speed/Duplex	Native VLAN	Trunk Mode	VLANs for Trunk Mode	
1/0	✓	✓	auto/auto	1	✓	--	
1/1	✓	✓	auto/auto	1	✓	--	
1/2	✓	✓	auto/auto	1	✓	--	
1/3	✓	✓	auto/auto	1	✓	--	

STP for all ports: Enabled NOTE: STP should be disabled if this Controller has only single uplink to the network

Back Next Cancel

- 9 Click **Next** twice, then click finish to save the changes to the configuration.
- 10 Enable igmp and local proxy ARP on the VLAN(s).
  - a. Navigate to **Configuration>NETWORK>IP**.
  - b. For each VLAN that supports handsets:
    - i. Click on **Edit** in the row representing the VLAN.
    - ii. Click on the **Enable IGMP** radio button.
    - iii. Ensure that **Enable IGMP Snooping** is unchecked.
    - iv. Check the **Enable IGMP Proxy** radio button.
    - v. Check the interfaces/ports that will have PTT multicast traffic flowing through them.

## *Creating Firewall Roles and Policies*

The Aruba MC has an application-aware stateful firewall that can assign prioritization to Spectralink voice traffic once it knows that a certain wireless client is a Spectralink handset. This is accomplished by the following steps:

- 1** Create a user role that the phones should be assigned to.
- 2** Create the syslog policy.
- 3** Assign firewall policies to the role.
- 4** Create a user-derivation rule that dictates how a client should be identified as a Spectralink voice phone. In this case it is easiest to classify based on the leading octets of the MAC OUI (00:90:7a).
- 5** Finally, create an AAA-profile that ties the user-derivation rule with the appropriate firewall rules.

## Creating a Syslog Policy

### On CLI

```
(Aruba651) (config) #ip access-list session syslog
```

```
(Aruba651) (config-sess-syslog) #any any svc-syslog permit
```

### On WebUI

- 1 Click the **Configuration** tab.
- 2 Click **Access Control**.
- 3 Click **Policies**.
- 4 Click **Add**.

The screenshot shows the Aruba Mobility Controller WebUI interface. The left sidebar contains a navigation menu with categories like WIZARDS, NETWORK, SECURITY, WIRELESS, MANAGEMENT, and ADVANCED SERVICES. The main content area is titled 'Security > Access Control > Firewall Policies'. Below this title are tabs for 'User Roles', 'System Roles', 'Policies', 'Time Ranges', and 'Guest Access'. The 'Policies' tab is active, showing a table of existing policies. The table has columns for 'Name', 'Type', 'Rule Count', 'Policy Usage', and 'Action'. Below the table is an 'Add' button.

Name	Type	Rule Count	Policy Usage	Action
validuser	session	3		<a href="#">Edit</a> <a href="#">Delete</a>
sys-control	session	9	sys-ap-role	<a href="#">Edit</a> <a href="#">Delete</a>
sys-ap-acl	session	10	sys-ap-role	<a href="#">Edit</a> <a href="#">Delete</a>
stateful-dot1x	session	2		<a href="#">Edit</a> <a href="#">Delete</a>
ap-uplink-acl	session	3		<a href="#">Edit</a> <a href="#">Delete</a>
allow-diskaervices	session	4		<a href="#">Edit</a> <a href="#">Delete</a>
allow-printservices	session	3		<a href="#">Edit</a> <a href="#">Delete</a>
control	session	10	ap-role	<a href="#">Edit</a> <a href="#">Delete</a>
logon-control	session	5	logon guest-logon	<a href="#">Edit</a> <a href="#">Delete</a>
ap-acl	session	6	ap-role	<a href="#">Edit</a> <a href="#">Delete</a>

1 2 3 Next | 1-10 of 28 [10]

[Add](#)

- 5 Set the Policy name to **syslog**, the policy type to **Session**, the service to **service**, the service name to **svc-syslog (udp-514)**, and the action to **permit**.



ARUBA  
NETWORKS

MOBILITY CONTROLLER | Aruba3600V1EW

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan Save Configuration Logout admin

WIZARDS  
AP Wizard  
Controller Wizard  
WLAN/LAN Wizard  
License Wizard

NETWORK  
Controller  
VLANs  
Ports  
Cellular Profile  
IP

SECURITY  
Authentication  
Access Control

WIRELESS  
AP Configuration  
AP Installation

MANAGEMENT  
General  
Administration  
Certificates  
SNMP  
Logging  
Clock  
Guest Provisioning  
Captive Portal  
SMTP  
Bandwidth Calculator

ADVANCED SERVICES  
Redundancy  
IP Mobility  
Stateful Firewall  
External Services  
VPN Services  
Wired Access  
Wireless  
All Profiles

**Security > Firewall Policies > Add New Policy**

User Roles System Roles **Policies** Time Ranges Guest Access

Policy Name syslog

Policy Type Session

Rules

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	Pause ARM Scanning	BlackList	Classify Media	TOS	802.1p Priority	Action
IPv4	any	any	Service	permit	<input type="checkbox"/>	<input type="checkbox"/>	Low		<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>			

Commands

View Commands

Apply

**6** Click **Add**, then **Apply**.

## Creating User-Role and Assigning Firewall Rules to the Role

### On CLI

```
(Aruba651) (config) #user-role spectralink
(Aruba651) (config-role) #access-list session sip-acl position 1
(Aruba651) (config-role) #access-list session tftp-acl position 2
(Aruba651) (config-role) #access-list session icmp-acl position 3
(Aruba651) (config-role) #access-list session dhcp-acl position 4
(Aruba651) (config-role) #access-list session syslog position 5
(Aruba651) (config-role) #access-list session dns-acl position 6
(Aruba651) (config-role) #access-list session lync-acl position 7
(Aruba651) (config-role) #access-list session http-acl position 8
(Aruba651) (config-role) #access-list session https-acl position 9
(Aruba651) (config-role) #access-list session ntp-acl position 10
(Aruba651) (config-role) #access-list session ftp-acl position 11
```



#### Admin Tip: Enter applications in firewall list

Ensure that applications installed on the phone are entered into the firewall list for the Spectralink role as needed.


### On WebUI

- 1 Click the **Configuration** tab.
- 2 Click **Access Control**.
- 3 Click **Add**
- 4 Assign a **Role-name** for the phones (Ex. spectralink).
- 5 Under **Firewall Policies**, click **Add**.
- 6 Click the **Choose** from configured policies radio-button.
- 7 From the drop down list select, **sip-acl**, **tftp-acl**, **icmp-acl**, **dhcp-acl**, **dns-acl**, **lync-acl**, **http-acl**, **https-acl**, **ntp-acl**, **ftp-acl**, and **syslog** policies to the list, clicking **Done** after each selection and repeating from step 5.
- 8 Click **Apply** at the bottom of the page.
- 9 Click **Save Configuration**.



### Admin Tip: Enter applications in firewall list

Ensure that applications installed on the phone are entered into the firewall list for the Spectralink role as needed.



Configuration

Monitoring Configuration Diagnostics Maintenance Plan Events Reports Licenses will expire in 28 days Save Configuration Logout admin

Wizards  
Controller Wizard  
WLAN Wizard  
License Wizard

Network  
Controller  
VLANs  
Ports  
IP

Security  
Authentication  
Access Control

Wireless  
AP Configuration  
AP Installation

Management  
General  
Administration  
Certificates  
SNMP  
Logging  
Clock

Advanced Services  
Redundancy  
IP Mobility  
Stateful Firewall  
Wired Access  
Wireless  
All Profiles

### Security > User Roles > Add Role

User Roles System Roles Policies Time Ranges Guest Access

Role Name: Polycom

Firewall Policies

Name	Rule Count	AP Group	Action
Add			

☒ Choose from Configured Policies:  AP Group:   
☐ Create New Policy From Existing Policy:    
☐ Create New Policy

Re-authentication Interval

Disabled  (0 disables re-authentication. A positive value enables authentication 0 - 4096 )

Role VLAN ID

Not Assigned

Bandwidth Contract

Upstream: Not Enforced  ☐ Per User

Downstream: Not Enforced  ☐ Per User

## Creating a User-Role Derivation Rule

### On CLI

```
(Aruba651) (config) # aaa derivation-rules user spectralink-derivation
(Aruba651) (user-rule) #set role condition macaddr starts-with 00:90:7a
set-value spectralink
(Aruba651) (user-rule) # write memory
```

### On WebUI

- 1 Click the **Configuration** tab.
- 2 Click **Authentication**.
- 3 Click **User Rules** and click **Add**.
- 4 Type a name for the user rules, such as spectralink-derivation.
- 5 Click **Add**.
- 6 Click the newly entered name in the tree in the left column.
- 7 Click **Add**.
- 8 Fill the following parameters
  - a **Set Type – Role**
  - b **Rule Type – MAC Address**
  - c **Condition – starts with**
  - d **Value – 00:90:7a**
  - e **Roles –** <select role created for phones> (spectralink in this example).
- 9 Click **Add** and then **Apply**.
- 10 Click **Save Configuration**.

Dashboard

Monitoring

Configuration

Diagnostics

Maintenance

Save Configuration

WIZARDS

AP

Controller

Campus WLAN

Remote AP

AirWave

NETWORK

Controller

VLANs

Ports

Cellular Profile

IP

SECURITY

> Authentication

Access Control

WIRELESS

AP Configuration

AP Installation

MANAGEMENT

General

Administration

Certificates

SNMP

Logging

Clock

Guest Provisioning

Captive Portal

SMTP

Bandwidth Calculator

Threshold

ADVANCED SERVICES

Redundancy

AirGroup

Security > Authentication > User Rules

ServersAAA ProfilesL2 AuthenticationL3 AuthenticationUser RulesAdvanced

User Rules Summary

spectralink-derivation

Rules-set: spectralink-derivation

Priority	Attribute	Operation	Operand	Action	Value	Total Hit	New Hit	Description	Actions
None found									

Add new rules

Set Type

Role

Rule Type

MAC Address

Condition

starts-with

Value

00:90:7a

Roles

ap-role

Description

spectralink

Add

Cancel

Configuration Updated Successfully.

Commands

View Commands

## Configuration Steps for None, WEP, WPA-PSK or WPA2-PSK Security

### Creating an Authentication Profile for controller-based authentication

#### On CLI

```
(Aruba651) (config) # aaa authentication dot1x default
```

#### Use the next four statements if using an external Radius server:

```
(Aruba651) (802.1X Authentication Profile "default") #termination enable
(Aruba651) (802.1X Authentication Profile "default") #termination eap-type
eap-tls
(Aruba651) (802.1X Authentication Profile "default") #termination eap-type
eap-peap
(Aruba651) (802.1X Authentication Profile "default") #termination inner-
eap-type eap-mschapv2
(Aruba651) (802.1X Authentication Profile "default") #exit

(Aruba651) (config) aaa authentication dot1x "spectralink-psk"
(Aruba651) (802.1X Authentication Profile "spectralink-psk") #machine-
authentication machine-default-role spectralink
(Aruba651) (802.1X Authentication Profile "spectralink-aaa") #machine-
authentication user-default-role spectralink
(Aruba651) (802.1X Authentication Profile "spectralink-aaa") #timer
idrequest_period 65535
(Aruba651) (802.1X Authentication Profile "spectralink-aaa")
#exit

(Aruba651) #configure terminal aaa profile spectralink-aaa
(Aruba651) (AAA Profile "spectralink-aaa") #initial-role authenticated
(Aruba651) (AAA Profile "spectralink-aaa") #authentication-dot1x
spectralink-psk
(Aruba651) (AAA Profile "spectralink-aaa") #user-derivation-rules
spectralink-derivation
```

#### On WebUI

- 1 Navigate to **Configuration** and **Authentication**.
- 2 Click the **L2-Authentication** tab.

- 3 Click **802.1X Authentication Profile** in the middle-pane to expand the tree and click **default**.
  - a On the right pane, check **Termination**. (Check these values if using an external Radius server.)
  - b For **Termination EAP-Type**, click **eap-peap** and **eap-tls**.
  - c For **Termination Inner EAP-Type**, check **eap-mschapv2**.
  - d Click **Apply**.

The screenshot shows the Aruba Spectralink VIEW configuration interface. The top navigation bar includes Dashboard, Monitoring, Configuration (active), Diagnostics, and Maintenance. A 'Save Configuration' button is visible. The left sidebar shows a tree structure with categories: WIZARDS, NETWORK, SECURITY, and WIRELESS. Under SECURITY, 'Authentication' is selected. The main pane is titled 'Security > Authentication > L2 Authentication'. It has tabs for Servers, AAA Profiles, L2 Authentication (active), L3 Authentication, User Rules, and Advanced. Under L2 Authentication, there is a tree view with 'MAC Authentication', '802.1X Authentication' (expanded), and 'Stateful 802.1X Authentication'. Under '802.1X Authentication', there are three sub-items: 'default', 'default-psk', and 'spectralink-802.1x' (selected). The right pane shows the configuration for '802.1X Authentication Profile > spectralink-802.1x'. It has tabs for 'Basic' and 'Advanced'. The 'Basic' tab is active, showing a table of configuration options:

Configuration Option	Value
Max authentication failures	0
Enforce Machine Authentication	<input type="checkbox"/>
Machine Authentication: Default Machine Role	spectralink
Machine Authentication: Default User Role	spectralink
Reauthentication	<input type="checkbox"/>
Termination	<input type="checkbox"/>
Termination EAP-Type	<input checked="" type="checkbox"/> eap-tls <input checked="" type="checkbox"/> eap-peap
Termination Inner EAP-Type	<input checked="" type="checkbox"/> eap-mschapv2 <input type="checkbox"/> eap-gtc

- 4 Click the **AAA Profiles** page and on the right-pane, click **Add**.
- 5 Assign a name to the AAA profile (Ex. spectralink-aaa) and click **Add**.
- 6 Click the newly created profile name.
- 7 Edit the AAA profile
  - a Drop-down the list against **User derivation rules** and select the rule created for the Spectralink phones.
  - b Click **Apply**.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration ⚡

WIZARDS

- AP
  - Controller
  - Campus WLAN
  - Remote AP
  - AirWave
- NETWORK
  - Controller
  - VLANs
  - Ports
  - Cellular Profile
  - IP
- SECURITY
  - > **Authentication**
    - Access Control
- WIRELESS
  - AP Configuration
  - AP Installation
- MANAGEMENT
  - General
  - Administration
  - Certificates
  - SNMP
  - Logging
  - Clock
  - Guest Provisioning
  - Captive Portal
  - SMTP
  - Bandwidth Calculator
  - Threshold
- ADVANCED SERVICES
  - Redundancy
  - AirGroup
  - IP Mobility
  - Stateful Firewall
  - External Services
  - VPN Services
  - Wired Access
  - All Profiles
  - [E-mail Support](#)

**Security > Authentication > Profiles**

Servers AAA Profiles **L2 Authentication** L3 Authentication User Rules Advanced

AAA

- default
- default-dot1x
  - MAC Authentication
    - MAC Authentication Server Group default
    - 802.1X Authentication default
    - 802.1X Authentication Server Group
    - RADIUS Accounting Server Group
  - XML API server
  - RFC 3576 server
- default-dot1x-psk
  - default-mac-auth
  - default-open
  - default-xml-api
  - NoAuthAAAProfile
- spectralink-aaa**
  - MAC Authentication
    - MAC Authentication Server Group default
    - 802.1X Authentication spectralink-psk
    - 802.1X Authentication Server Group
    - RADIUS Accounting Server Group
  - XML API server
  - RFC 3576 server
  - spectralink-dot1x

**AAA Profile > spectralink-aaa** Show Reference Save As Reset

Initial role	authenticated
MAC Authentication Default Role	guest
802.1X Authentication Default Role	guest
L2 Authentication Fail Through	<input type="checkbox"/>
User idle timeout	<input type="checkbox"/> Enable seconds
RADIUS Interim Accounting	<input type="checkbox"/>
User derivation rules	spectralink-derivation
Wired to Wireless Roaming	<input checked="" type="checkbox"/>
SIP authentication role	--NONE--
Device Type Classification	<input checked="" type="checkbox"/>
Enforce DHCP	<input type="checkbox"/>

Commands Apply View Commands

- 8 Click on **802.1X Authentication** underneath the **spectralink-aaa** profile entry.
  - a Click the **Advanced** tab.
  - b By **802.1X Authentication Profile**, click on **--NEW--**.
  - c Enter a name in the box by **--NEW--**, **spectralink-psk**.
  - d From the drop down list by **Machine Authentication: Default Machine Role**, select the role created earlier, **spectralink**.
  - e From the drop down list by **Machine Authentication: Default User Role**, select the role created earlier, **spectralink**.
  - f Set the Interval between Identity Requests to **65535**.
  - g Click **Apply**.
  - h Click **Save Configuration**.



Dashboard | Monitoring | **Configuration** | Diagnostics | Maintenance | Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave

NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP

SECURITY  
 > **Authentication**  
 Access Control

WIRELESS  
 AP Configuration  
 AP Installation

MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP

Bandwidth Calculator  
 Threshold

ADVANCED SERVICES  
 Redundancy  
 AirGroup  
 IP Mobility  
 Stateful Firewall  
 External Services  
 VPN Services  
 Wired Access  
 All Profiles  
[E-mail Support](#)

**Security > Authentication > Profiles**

Servers | **AAA Profiles** | L2 Authentication | L3 Authentication | User Rules | Advanced

AAA  
 default  
 default-dot1x  
 MAC Authentication  
 MAC Authentication Server Group default  
 802.1X Authentication default  
 802.1X Authentication Server Group  
 RADIUS Accounting Server Group  
 XML API server  
 RFC 3576 server  
 default-dot1x-psk  
 default-mac-auth  
 default-open  
 default-xml-api  
 NoAuthAAAProfile  
 spectralink-aaa  
 MAC Authentication  
 MAC Authentication Server Group default  
 802.1X Authentication spectralink-psk  
 802.1X Authentication Server Group  
 RADIUS Accounting Server Group  
 XML API server  
 RFC 3576 server  
 spectralink-dot1x

**802.1X Authentication Profile > spectralink-psk** Show Reference Save As Reset

Basic | Advanced

Max authentication failures	0
Enforce Machine Authentication	<input type="checkbox"/>
Machine Authentication: Default Machine Role	spectralink
Machine Authentication Cache Timeout	24 hr(s)
Blacklist on Machine Authentication Failure	<input type="checkbox"/>
Machine Authentication: Default User Role	spectralink
Interval between Identity Requests	65535 sec
Quiet Period after Failed Authentication	30 sec
Reauthentication Interval	86400 sec
Use Server provided Reauthentication Interval	<input type="checkbox"/>
Use the termination-action attribute from the Server	<input type="checkbox"/>
Multicast Key Rotation Time Interval	1800 sec
Unicast Key Rotation Time Interval	900 sec
Authentication Server Retry Interval	5 sec
Authentication Server Retry Count	3
Framed MTU	1100 bytes
Number of times ID-Requests are retried	5
Maximum Number of Reauthentication Attempts	3
Maximum number of times Held State can be bypassed	0
Dynamic WEP Key Message Retry Count	1
Dynamic WEP Key Size	128 bits
Interval between WPA/WPA2 Key Messages	1000 msec
Delay between EAP-Success and WPA2 Unicast Key Exchange	0 msec
Delay between WPA/WPA2 Unicast Key and Group Key Exchange	0 msec
Time interval after which the PMKSA will be deleted	8 hr(s)
Delete Keycache upon user deletion	<input type="checkbox"/>
WPA/WPA2 Key Message Retry Count	3
Multicast Key Rotation	<input type="checkbox"/>
Unicast Key Rotation	<input type="checkbox"/>

Apply

**Commands** View Commands

## Configuration Steps for WPA2-Enterprise Security

### Defining an 802.1X authentication server

#### On CLI

```
(Aruba651) (config) #aaa authentication-server radius <server-group name>
(Aruba651) (RADIUS Server "spectralink-dot1x") #host <server IP>
(Aruba651) (RADIUS Server "spectralink-dot1x") #key <RADIUS secret>
(Aruba651) (RADIUS Server "spectralink-dot1x") #write memory
```

#### On WebUI

- 1 Navigate to **Configuration** and **Authentication**.
- 2 Click **RADIUS Server**, name server profile (Ex. Spectralink-dot1x) and click **Add**.
- 3 Click the newly created instance to configure.
- 4 Input the IP address of the external RADIUS server and the pre-shared key.



#### **Settings: Define Aruba Controller on Radius with the same secret**

The Aruba mobility controller should be defined as a dot1x client on the RADIUS server and configured with the same secret as in step 4 above.

- 5 Click **Apply** and **Save Configuration**.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave

NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP

SECURITY  
**> Authentication**  
 Access Control

WIRELESS  
 AP Configuration  
 AP Installation

MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold

ADVANCED SERVICES  
 Redundancy  
 AirGroup  
 IP Mobility

**Security > Authentication > Servers**

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

Server Group  
 RADIUS Server  
 CiscoACS

LDAP Server  
 Internal DB  
 Tacacs Accounting Server  
 TACACS Server  
 XML API Server  
 RFC 3576 Server  
 Windows Server

**RADIUS Server > CiscoACS** Show Reference Save As Reset

Host 172.29.65.19

Key  
 Retype:

Auth Port 1812

Acct Port 1813

Retransmits 3

Timeout 5 sec

NAS ID

NAS IP

Enable IPv6 ☐

NAS IPv6

Source Interface vlanid ipv6addr

Use MD5 ☐

Use IP address for calling station ID ☐

Mode ☒

Lowercase MAC addresses ☐

MAC address delimiter none

Service-type of FRAMED-USER ☐

Commands Apply View Commands



## Settings: Define OKC on the 84-Series and 8020/8030 handsets

**Fast roaming** must be set to **Opportunistic Key Caching (OKC)** on the handset when WPA2-Enterprise is in use. It is enabled by default on the controller. The 87-Series handsets automatically detect the type of fast roaming necessary.

## Create a Server Group and Add the RADIUS Server

### Using CLI

```
(Aruba651) #configure terminal
(Aruba651) (config) #aaa server-group < Server Name > (Ex.Spectralink)
(Aruba651) (Server Group "Spectralink") # auth-server "Spectralink-dot1x"
position 1
(Aruba651) (Config) #aaa profile "Spectralink-dot1x"
(Aruba651) (AAA Profile ""Spectralink-dot1x") #dot1x-server-group
"Spectralink"
```

### Using WebUI

- 1 Navigate to **Configuration** and **Authentication**.
- 2 Click the **Servers** tab. Click the **Server Group**.
- 3 In the right pane click **Add** and create a new server group (Ex. Spectralink).
- 4 Click the newly created server group.
- 5 Click **New** under Servers tab.
- 6 Assign the required RADIUS server under Server Name, click **Add Server** and **Apply** button.

## Creating an 802.1X Authentication Profile

### Using CLI

```
(Aruba651) (config) #aaa authentication dot1x <profile-name>
```

If termination is required (the Radius server is external)

```
(Aruba651) (802.1X Authentication Profile "spectralink-dot1x") #termination enable
```

```
(Aruba651) (802.1X Authentication Profile "spectralink-dot1x") #termination eap-type eap-peap
```

```
(Aruba651) (802.1X Authentication Profile "spectralink-dot1x") #termination eap-type eap-tls
```

```
(Aruba651) (802.1X Authentication Profile "spectralink-dot1x") #termination inner-eap-type eap-mschapv2
```

### Using WebUI

- 1 Navigate to **Configuration** and **Authentication**.
- 2 Click the **L2 Authentication** tab.
- 3 Click **Add** and create a new profile (Ex. spectralink-dot1x).
- 4 Click **802.1X Authentication Profile**.
- 5 Click the newly created instance and enable termination. Specify the **EAP type** to be **eap-peap** and **eap-tls** and the **Inner-EAP type** to be **eap-mschapv2**.
- 6 Click **Apply** and **Save Configuration**.

The screenshot displays the Aruba Spectralink WebUI interface. The top navigation bar includes tabs for Dashboard, Monitoring, Configuration (selected), Diagnostics, and Maintenance. A 'Save Configuration' button is visible on the right. The left sidebar shows a tree view with categories: WIZARDS, NETWORK, SECURITY, and WIRELESS. Under SECURITY, 'Authentication' is selected. The main content area is titled 'Security > Authentication > L2 Authentication'. It features several tabs: Servers, AAA Profiles, L2 Authentication (selected), L3 Authentication, User Rules, and Advanced. Under the L2 Authentication tab, there are two main sections: 'MAC Authentication' and '802.1X Authentication'. The '802.1X Authentication' section is expanded, showing a list of profiles: 'default', 'default-psk', 'spectralink-802.1x' (selected), and 'spectralink-psk'. The 'spectralink-802.1x' profile is selected, and its configuration is shown in a modal window titled '802.1X Authentication Profile > spectralink-802.1x'. This modal has two tabs: 'Basic' and 'Advanced'. The 'Basic' tab is active, showing the following configuration: 'Max authentication failures' is set to 0; 'Enforce Machine Authentication' is unchecked; 'Machine Authentication: Default Machine Role' is set to 'spectralink'; 'Machine Authentication: Default User Role' is set to 'spectralink'; 'Reauthentication' is unchecked; 'Termination' is unchecked; 'Termination EAP-Type' has checkboxes for 'eap-tls' and 'eap-peap' (both checked); 'Termination Inner EAP-Type' has checkboxes for 'eap-mschapv2' (checked) and 'eap-gtc' (unchecked). Buttons for 'Show Reference', 'Save As', and 'Reset' are located at the top right of the modal.

## Creating an Authentication Profile

### Using CLI

```
(Aruba651) #configure terminal aaa profile <profile-name>
(Aruba651) (AAA Profile "spectralink-dot1x") #authentication-dot1x <post-
authentication role name>
(Aruba651) (AAA Profile "spectralink-dot1x") #dot1x-server-group <dot1x
authentication server name>
```

### Using WebUI

- 1 Navigate to **Configuration** and **Authentication**.
- 2 Click the **AAA Profiles** tab.
- 3 Click **Add** and create a new profile (Ex. spectralink-dot1x).
- 4 Expand the newly created profile.
- 5 Change the **User derivation rules** (Ex. spectralink-derivation) to the user-role created for the phones.
- 6 Click **802.1X Authentication Profile** and specify the newly created profile.
- 7 Click **Apply** and **Save Configuration**.

ARUBA networks MOILITY CONTROLLER | Aruba3600 [Log out admin](#)

Dashboard Monitoring **Configuration** Diagnostics Maintenance [Save Configuration](#)

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave  
 NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP  
 SECURITY  
**> Authentication**  
 Access Control  
 WIRELESS  
 AP Configuration  
 AP Installation  
 MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold  
 ADVANCED SERVICES  
 Redundancy

**Security > Authentication > Profiles**

Servers AAA Profiles **L2 Authentication** L3 Authentication User Rules Advanced

MAC Authentication

MAC Authentication Server Group default

802.1X Authentication default -psk

802.1X Authentication Server Group

RADIUS Accounting Server Group

XML API server

RFC 3576 server

default-mac-auth

default-open

default-xml-api

NoAuthAAAProfile

spectralink-aaa

**spectralink-dot1x**

MAC Authentication

MAC Authentication Server Group default

802.1X Authentication spectralink -802.1x

802.1X Authentication Server Group RADIUS

RADIUS Accounting

**AAA Profile > spectralink-dot1x** [Show Reference](#) [Save As](#) [Reset](#)

Initial role logon

MAC Authentication Default Role guest

802.1X Authentication Default Role guest

L2 Authentication Fail Through ☐

User idle timeout ☐ Enable seconds

RADIUS Interim Accounting ☐

User derivation rules spectralink-derivation

Wired to Wireless Roaming ☒

SIP authentication role --NONE--

Device Type Classification ☒

Enforce DHCP ☐

[Apply](#) [View Commands](#)

**Commands**

## Wireless LAN Configuration

This section defines the wireless network parameters that are most aptly suited to the Spectralink phones.

It is required to have separate SSID for the Spectralink phones and other data clients. Also, certain parameters need to be modified to allow seamless interoperability of Spectralink phones in and out of call with Aruba's Adaptive Radio Management (ARM) mechanism. Aruba OS accomplishes this by creating independent profiles for the SSID definition, radio definition and ARM definitions before tying them together to an AP-group on which they would operate. This way, all APs configured to be part of the AP-group will have the same operational parameters. The steps in this procedure are below

- 1 Create an SSID profile – each SSID profile is characterized by the ESSID and the authentication-encryption scheme.
- 2 Create a VOIP CaC profile that defines the bandwidth limits for calls per AP.
- 3 Create a HT-SSID profile (with 802.11n features enabled or disabled as appropriate for the deployed network) and assign the HT-SSID to the SSID profile.
- 4 Create a Virtual-AP profile that ties the SSID profile and authentication profile (created in the previous section) with a VLAN on the wired-side.
- 5 Create a Traffic Management Profile that allocates all of the bandwidth tracked by bandwidth control to the virtual AP profile defined for voice. (Other clients will have their own virtual AP profiles with their own tracking.)
- 6 Create Radio-profiles for the 2.4 GHz and 5 GHz radio. This would include ARM and HT-Radio profile settings. In this example, we modify the default radio profiles which are assigned to the Virtual-AP automatically.
- 7 Associate the Virtual-AP with an AP-group.

The WLAN configuration for 802.1X authentication is identical to that for PSK-based authentication except for the following 2 points

- In Creating a SSID-profile, encryption (opmode) on the SSID should be set to **wpa2-aes**.
- The AAA profile for the Virtual-AP should be set to the newly created **dot1x** profile (spectralink-dot1x).

### On CLI

#### Creating a SSID-profile

```
(Aruba651) #configure terminal wlan ssid-profile view
```

```
For None (open network - no security) #opmode opensystem
```

```
For WEP
```



```
(Aruba651) (SSID Profile "view") #opmode static-wep
(Aruba651) (SSID Profile "view") #weptxkey <index 1-4>
(Aruba651) (SSID Profile "view") #wepkey<index> <"string of hex
characters">
```

For WPA-PSK

```
(Aruba651) (SSID Profile "view") #opmode wpa-psk-tkip
(Aruba651) (SSID Profile "view") #wpa-passphrase <"passphrase">
```

For WPA2-PSK

```
(Aruba651) (SSID Profile "view") #opmode wpa2-aes-psk
(Aruba651) (SSID Profile "view") #wpa-passphrase < "passphrase">
```

For all

```
(Aruba651) (SSID Profile "view") #dtim-period 2
(Aruba651) (SSID Profile "view") #wmm
(Aruba651) (SSID Profile "view") #wmm-uapsd
(Aruba651) (SSID Profile "view") #max-retries 8
(Aruba651) (SSID Profile "view") #max-tx-fail 0
(Aruba651) (SSID Profile "view") #wmm-vi-dscp 40
(Aruba651) (SSID Profile "view") #wmm-vo-dscp 46
(Aruba651) (SSID Profile "view") #wmm-be-dscp 0
(Aruba651) (SSID Profile "view") #wmm-bk-dscp 0
(Aruba651) (SSID Profile "view") #no wmm-override-dscp-mapping
(Aruba651) (SSID Profile "view") #wmm-ts-min-inact-in 3600000
(Aruba651) (SSID Profile "view") #no strict-svp
(Aruba651) (SSID Profile "view") #essid view
(Aruba651) (SSID Profile "view") #a-tx-rates 6 9 12 18 24 36 48 54
(Aruba651) (SSID Profile "view") #g-basic-rates 5 11
(Aruba651) (SSID Profile "view") #g-tx-rates 5 6 11 12 18 24 36 48 54
(Aruba651) (SSID Profile "view") #max-tx-fail 0
```

## Creating a Virtual-AP

```
(Aruba651) #configure terminal wlan virtual-ap spectralink-vap
(Aruba651) (Virtual AP Profile "spectralink-vap") #no broadcast-filter arp
(Aruba651) (Virtual AP Profile "spectralink-vap") #vlan 1
```

## Creating a VoIP CAC profile

In the CLI commands below, use the bandwidth from the table below that corresponds to the codec the phones on the network will be using. As described in *Spectralink 84-Series Wireless Telephone Administration Guide*, the 84-Series handsets support the codecs shown in the table below. If the configuration is not changed from the default described in the reference, the codec used will be the one shown first in the table that is supported by the other side of the call. The 84-Series handsets can be configured to add the optional codecs shown in the table. This feature is used when communicating with desksets with high definition audio.

The 8020/8030 phones support G.711 $\mu$ -law, G.711a-law and G.729 codecs but always ask for the largest bandwidth allocation, so only one entry is needed per radio band.

Choose the bandwidth from the table below that is the smallest number needed to support the type of phones or codecs expected so that the number of calls will be limited to what the AP can support.



### Admin Tip: 87-Series, WMM-AC Incompatible

Spectralink 87-Series handsets have not yet implemented TSPEC control. They will not operate properly in a network with WMM-AC turned on.

#### 8020/8030 handsets

Codec	Radio	Bandwidth
All	5.0 GHz	1500
All	2.4 GHz	1100

#### 84-Series handsets Default Codecs (in priority order)

Codec	Radio	Bandwidth
G.722	5.0 GHz	3200
G.722	2.4 GHz	2000
G.722.1 (32 kbps)	5.0 GHz	2000
G.722.1 (32 kbps)	2.4 GHz	1600
G.711Mu-law	5.0 GHz	3200
G.711Mu-law	2.4 GHz	2400

<i>Codec</i>	<i>Radio</i>	<i>Bandwidth</i>
G.711A-law	5.0 GHz	3200
G.711A-law	2.4 GHz	2400
G.729AB	5.0 GHz	1200
G.729AB	2.4 GHz	1000

#### 84-Series Handsets Configurable Codecs

<i>Codec</i>	<i>Radio</i>	<i>Bandwidth</i>
G.722.1 (16 kbps)	5.0 GHz	1400
G.722.1 (16 kbps)	2.4 GHz	1000
G.722.1 (24 kbps)	5.0 GHz	1800
G.722.1 (24 kbps)	2.4 GHz	1400
L16.8 (128 kbps)	5.0 GHz	6000
L16.8 (128 kbps)	2.4 GHz	4700
L16.16 (256 kbps)	5.0 GHz	5800
L16.16 (256 kbps)	2.4 GHz	4400

### Generally disable deep packet inspection if CAC is enabled

```
(Aruba651)# configure terminal
(Aruba651)# voice alg-based-cac disable
(Aruba651)# wlan voip-cac-profile "8400_g"
(Aruba651) (VoIP Call Admission Control profile "8400_g") #call-admission-
control
(Aruba651) (VoIP Call Admission Control profile "8400_g") #bandwidth-cac
(Aruba651) (VoIP Call Admission Control profile "8400_g") #bandwidth-capacity
2400
(Aruba651) (VoIP Call Admission Control profile "8400_g") #wmm-tspec-
enforcement-period 3
```

```
(Aruba651) (VoIP Call Admission Control profile "8400_g") #send-sip-status-
code client none
(Aruba651) (VoIP Call Admission Control profile "8400_g") #send-sip-status-
code server none
```

### Changing AP EDCA profile

```
(Aruba651) #configure terminal wlan edca-parameter-profile ap AC_ON
(Aruba651) # video acm 1
(Aruba651) # voice acm 1
```

Or

```
(Aruba651) #configure terminal wlan edca-parameter-profile ap AC_OFF
(Aruba651) # video acm 0
(Aruba651) # voice acm 0
```

Note: turn acm to 1 only if 87-Series handsets are not present in the network

### Changing station EDCA profile

```
(Aruba651) #configure terminal wlan edca-parameter-profile station AC_ON
(Aruba651) # video acm 1
(Aruba651) # voice acm 1
```

Or

```
(Aruba651) #configure terminal wlan edca-parameter-profile station AC_OFF
(Aruba651) # video acm 0
(Aruba651) # voice acm 0
```

Note: turn acm to 1 only if 87-Series handsets are not present in the network

### HT-SSID profile (disable 802.11n network)

```
(Aruba651) #configure terminal wlan ht-ssid-profile ht-disabled
(Aruba651) (High-throughput SSID profile "ht-disabled") #no high-
throughput-enable
(Aruba651) (High-throughput SSID profile "ht-disabled") #no 40MHz-enable
(Aruba651) (High-throughput SSID profile "ht-disabled") #no mpdu-agg
```

### HT-SSID profile (enable 802.11n network)

```
(Aruba651) #configure terminal wlan ht-ssid-profile ht-enabled
(Aruba651) (High-throughput SSID profile "ht-enabled") #high-throughput-
enable
```

For 12x and 13x APs, set the maximum number of MSDUs in an A-MSDU on best-effort AC and the maximum number of MSDUs in an A-MSDU on background AC both to 10. For 11n APs with model numbers smaller than 12x, set these values to 3.

Set the Maximum number of MSDUs in an A-MSDU on video AC and Maximum number of MSDUs in an A-MSDU on voice AC both to 3.



#### **Admin Tip: A-MSDU Aggregation Settings**

The AP-125 and AP-135 and newer AP's can process 10 packets per background and best effort aggregation. Older 11n AP's have better performance with a setting of 3 packets per background and best effort aggregation. Voice and video should remain with 3 packets per aggregation to avoid audible/visible latency issues.



#### **Admin Tip: Disable A-MPDU on handset SSIDs**

The Spectralink handsets do not implement A-MPDU aggregation. They cause extra traffic by declining Block ACK requests. It eliminates extra traffic to disable A-MPDU traffic on SSIDs used for handset traffic.

```
(Aruba651) (High-throughput SSID profile "ht-enabled") #max-tx-a-msdu-count-be <3 or 10, depending on AP model>
```

```
(Aruba651) (High-throughput SSID profile "ht-enabled") #max-tx-a-msdu-count-bk <3 or 10, depending on AP model>
```

```
(Aruba651) (High-throughput SSID profile "ht-enabled") #max-tx-a-msdu-count-vi 3
```

```
(Aruba651) (High-throughput SSID profile "ht-enabled") #max-tx-a-msdu-count-vo 3
```

```
(Aruba651) (High-throughput SSID profile "ht-enabled") #no mpdu-agg
```

For 80 MHz network

```
(Aruba 3600) (High-throughput SSID profile "ht-enabled") #80-MHz-enable
```

Note: the AP must be power cycled for the 80 MHz setting to take effect.

For 40 MHz network:

```
(Aruba651) (High-throughput SSID profile "ht-enabled") #40MHz-enable
```

```
(Aruba 3600) (High-throughput SSID profile "ht-enabled") #no 80-MHz-enable
```

For 20 MHz network

```
(Aruba651) (High-throughput SSID profile "ht-enabled") #no 40MHz-enable
```

```
(Aruba651) (High-throughput SSID profile "ht-enabled") #no 80MHz-enable
```

```
(Aruba651) (High-throughput SSID profile "ht-enabled")
```



### Admin Tip: Paired channel recommendation

40 MHz (paired) channels are not recommended by Aruba on the 2.4 GHz radio band.

```
(Aruba651) (High-throughput SSID profile "ht-enabled") #mpdu-agg
```

```
If WEP or no security is desired to be allowed (Aruba651) (High-throughput SSID profile "ht-enabled") #allow-weak-encryption
```

### Assigning HT-SSID and EDCA profiles to the SSID-Profile

```
(Aruba651) #configure terminal wlan ssid-profile view
```

```
(Aruba651) (SSID Profile "view") #ht-ssid-profile <ht-disabled or ht-enabled>
```

```
(Aruba651) (SSID Profile "view") #edca-parameters-profile station <AC_OFF or AC_ON>
```

```
(Aruba651) (SSID Profile "view") #edca-parameters-profile ap <AC_OFF or AC_ON>
```

### Adding the aaa-profile and the ssid-profile to the virtual-ap profile

```
(Aruba651) (config) #wlan virtual-ap spectralink-vap
```

```
(Aruba651) (Virtual AP profile "spectralink-vap") #aaa-profile spectralink-aaa
```

```
(Aruba651) (Virtual AP profile "spectralink-vap") #ssid-profile spectralink-dot1x
```

### Creating Traffic Management Profiles

```
(Aruba651)# configure terminal wlan dot11a-traffic-management-profile "AC_ON"
```

```
(Aruba651) (traffic-management-profile "AC_ON") #bw-alloc virtual-ap "spectralink-vap" share 100 enforcement hard
```

```
(Aruba651) (traffic-management-profile "AC_ON") #report-interval 1
```

### Creating Radio profiles

In most cases, one can use the default Radio-profile, HT-Radio profile and ARM profile and modify them as required. If there are multiple AP-groups on the network that require different radio profiles, please refer to the ArubaOS User Guide to create and assign radio-profiles to AP-Groups.

#### 5 GHz Radio settings

```
(Aruba651) (config) #rf dot11a-radio-profile default
```

#### Enable or disable 5 GHz radio

```
(Aruba651) (802.11a radio profile "default") #<no> radio-enable
```

**Choose a channel**

```
(Aruba651) (802.11a radio profile "default")#channel <desired channel>
```

**Enable 80 MHz or not**

```
(Aruba651) (802.11a radio profile "default")#<no> very-high-throughput  
enable
```

**Enable 40 MHz or not**

```
(Aruba651) (802.11a radio profile "default")#<no> high-throughput enable
```

**Admin Tip: Transmit Power**

For setting up the **Transmit Power**, please consult your facility's RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. Spectralink Wireless Telephones require the following minimum dBm reading to support the corresponding **Mandatory** data rate setting in the access point.

<i>802.11 Radio Standard</i>	<i>Minimum Available Signal Strength (RSSI)</i>	<i>Maximum "Mandatory" Data Rate</i>
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s

**Web Info: RF Deployment reference**

For additional details on RF deployment please see the *Deploying Enterprise-Grade Wi-Fi Telephony* White Paper.

```
(Aruba651) (802.11a radio profile "default")#tx-power <transmit EIRP in .5  
dBm increments)
```

```
(Aruba651) (802.11a radio profile "default")#no spectrum-load-balancing
```

```
(Aruba651) (802.11a radio profile "default")#cap-reg-eirp 0
```

If DFS channels (shared with radar) are used on 802.11a/n radio, the following commands to alter the default radio profile or other defined radio profile will be necessary

```
(Aruba651) (802.11a radio-profile "default") #csa
```

```
(Aruba651) (802.11a radio-profile "default") #csa-count 4
```

```
(Aruba651) (802.11a radio-profile "default") #dot11h
```

**2.4 GHz Radio settings**

```
(Aruba651) (config) #rf dot11g-radio-profile default
```

**Enable or disable 2.4 GHz radio**

```
(Aruba651) (802.11g radio profile "default")#<no> radio-enable
```

#### Choose a channel

```
(Aruba651) (802.11g radio profile "default")#channel <desired channel>
```

#### Disable 40 MHz

```
(Aruba651) (802.11b radio profile "default")#<no> high-throughput enable
```



#### Admin Tip: Transmit Power

For setting up the **Transmit Power**, please consult your facility's RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. Spectralink Wireless Telephones require the following minimum dBm reading to support the corresponding **Mandatory** data rate setting in the access point.

<i>802.11 Radio Standard</i>	<i>Minimum Available Signal Strength (RSSI)</i>	<i>Maximum "Mandatory" Data Rate</i>
802.11b	-65 dBm	11 Mb/s
802.11g	-67 dBm	6 Mb/s
802.11g	-47 dBm	54 Mb/s



#### Web Info: RF Deployment reference

For additional details on RF deployment please see the *Deploying Enterprise-Grade Wi-Fi Telephony* White Paper.

```
(Aruba651) (802.11g radio profile "default")#tx-power <transmit EIRP in .5 dBm increments>
```

```
(Aruba651) (802.11g radio profile "default")#no spectrum-load-balancing
```

```
(Aruba651) (802.11g radio profile "default")#cap-reg-eirp 0
```

#### If using 8020/8030 phones or other devices that are not n-enabled

```
(Aruba651)# config terminal rf ht-radio-profile default-a
```

```
(Aruba651) (High-throughput radio profile "default-a") #CSD-override
```

```
(Aruba651)# exit
```

```
(Aruba651) (config)#rf ht-radio-profile default-g
```

```
(Aruba651) (High-throughput radio profile "default-g") #CSD-override
```



## Assigning the HT Radio Profiles to the Virtual AP

```
(Aruba651)# config terminal wlan virtual-ap spectralink-vap
(Aruba651) (Virtual AP profile "spectralink-vap") #configure terminal rf
ht-radio-profile default-g
(Aruba651) (Virtual AP profile "spectralink-vap") #configure terminal rf
ht-radio-profile default-a
```

## Creating an ARM profile

```
(Aruba 3600) #configure terminal rf arm-profile default
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default")
#assignment <disable or maintain >
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # voip-
aware-scan
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # 40MHz-
allowed All
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # client-
aware
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # no
active-scan
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # ota-
updates
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # scanning
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # multi-
band-scan
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # voip-
aware-scan
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # power-
save-aware scan
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # video-
aware-scan
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # no
client-match
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # write
memory
```

## Assigning properties to an AP-Group

### Virtual AP assignment

```
(Aruba651) #configure terminal ap-group default
(Aruba651) (AP group "default") #virtual-ap spectralink-vap
(Aruba651) (AP group "default") #voip-cac-profile "8400_g"
(Aruba651) (AP group "default") #dot11a-traffic-mgmt-profile "AC_ON"
```

```
(Aruba651) (AP group "default") #dot11g-traffic-mgmt-profile "AC_ON"
```

Normally, one would have to assign the Radio-profile to an AP-Group. But this example uses the default radio profiles which are assigned to the default AP-Group automatically.

## On WebUI

### Creating a Virtual-AP

- 1 Navigate to **Configuration** and **AP Configuration**.
- 2 Click **Edit** against the default **AP-Group**.
- 3 Click **Wireless LAN** and **Virtual AP**.
- 4 Click **Add**.
- 5 On the right-pane, select **NEW** under **Add a profile** and enter a profile name (Ex., spectralink-vap) and click **Add**.
- 6 Click on the newly entered name and enter the following options
  - a Check **Virtual AP enable**.
  - b Allowed band – **all** (or select a band, if the design calls for voice on only one band).
  - c Select the VLAN where the voice handsets would reside.
  - d In the right pane, uncheck Convert Broadcast ARP requests to unicast.
  - e Click **Apply**.

Dashboard | Monitoring | **Configuration** | Diagnostics | Maintenance | Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave  
 NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP  
 SECURITY  
 Authentication  
 Access Control  
 WIRELESS  
 > **AP Configuration**  
 AP Installation  
 MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold  
 ADVANCED SERVICES  
 Redundancy  
 AirGroup  
 IP Mobility  
 Stateful Firewall

**Configuration > AP Group > Edit "default"**

Profiles	Profile Details
<ul style="list-style-type: none"> <li>Wireless LAN               <ul style="list-style-type: none"> <li>Virtual AP                   <ul style="list-style-type: none"> <li>cac</li> <li>VPSK</li> <li><b>spectralink-vap</b></li> </ul> </li> <li>AAA spectralink-dot1x</li> <li>802.11K default</li> <li>Hotspot 2.0 default</li> <li>SSID view</li> <li>WMM Traffic Management</li> <li>ADYS</li> <li>RF Management                   <ul style="list-style-type: none"> <li>AP</li> <li>QOS</li> <li>IDS</li> <li>Mesh</li> </ul> </li> </ul> </li> </ul>	<b>Virtual AP &gt; spectralink-vap</b> Show Reference Save As Reset Basic Advanced Virtual AP enable <input checked="" type="checkbox"/> VLAN <input type="text"/> Forward mode tunnel Allowed band all Band Steering <input type="checkbox"/> Steering Mode prefer-5ghz Dynamic Multicast Optimization (DMO) <input type="checkbox"/> Dynamic Multicast Optimization (DMO) Threshold 5 Drop Broadcast and Multicast <input type="checkbox"/> Convert Broadcast ARP requests to unicast <input type="checkbox"/> Authentication Failure Blacklist Time 3600 sec Blacklist Time 3600 sec Deny inter user traffic <input type="checkbox"/> Deny time range --NONE-- DoS Prevention <input type="checkbox"/> HA Discovery on-association <input checked="" type="checkbox"/> Mobile IP <input checked="" type="checkbox"/> Preserve Client VLAN <input type="checkbox"/> QinQ Outer VLAN 0 Remote-AP Operation standard Station Blacklisting <input checked="" type="checkbox"/> Strict Compliance <input type="checkbox"/> VLAN Mobility <input type="checkbox"/> Apply

## Creating a SSID-profile

- 1 Click the newly created virtual-ap in the left-hand Virtual AP list.
- 2 Click **SSID profile**.
  - a On the right pane, select **NEW** and enter an SSID-profile name (Ex., spectralink).
  - b Enter the desired SSID-name.
  - c When Spectralink phones are configured for None (not recommended, but useful for provisioning), under **Network Authentication**, select **None**, and under **Encryption**, select **Open**.
  - d When Spectralink phones are configured for WEP, under **Network Authentication**, select **None**, and under **Encryption**, select **WEP**. For the 40 Bits key on the Spectralink phone, use the 64-bit key Aruba setting, entering 10 hex digits. For the 104-bit key on the Spectralink phone, use the 128-bit key Aruba setting, entering 26 hex digits.
  - e WPA-PSK is no longer available through the Web GUI. It must be entered with the following cli commands:

```
(Aruba651) #configure terminal wlan ssid-profile view
(Aruba651) (SSID Profile "view") #opmode wpa-psk-tkip
(Aruba651) (SSID Profile "view") #wpa-passphrase <"passphrase">
```

- f When Spectralink phones are configured for WPA2-PSK under **Network Authentication**, select **WPA2-PSK** and **Open** under **Encryption**. Enter a preshared key in either Hex or as a passphrase.
  - g When Spectralink phones are configured for WPA2-Enterprise, under **Network Authentication** select **WPA2** and **AES** under **Encryption**.
  - h Click **Apply**
- 3 Click the **Advanced** tab on the right pane.
  - a Make the following changes
  - b **DTIM Interval** – 2
  - c **802.11g transmit rates** – check 5, 6, 9, 11, 12, 18, 24, 36, 48, 54.
  - d **802.11g basic rates** – check 5, 11
  - e **802.11a transmit rates** – check, 6, 9, 12, 18, 24, 36, 48, 54.
  - f **802.11a basic rates** – check 6, 12, 24
  - g Check **Wireless Multimedia (WMM)**.
  - h Check **Wireless Multimedia U-APSD (WMM-UAPSD) Powersave**
  - i Set **Max Transmit Attempts** to 8.
  - j Set **DSCP mapping for WMM voice AC** to 46 to match Spectralink phone setting
  - k Set **DSCP mapping for WMM video AC** to 40 to match Spectralink phone setting
  - l Set **WMM TSPEC** inactivity interval to 3600000 msec.
  - m Set DSCP mapping for WMM best-effort AC to 0.
  - n Set DSCP mapping for background AC to 0.
  - o Ensure that **Override DSCP mappings for WMM clients** is NOT checked.
  - p Ensure that **Maximum Transmit Failures** is set to 0 to disable deauthentication of the handsets when acks are not received.
  - q Ensure that **Enable OKC** is checked, if the option is given in the controller software version in use.
- 4 Click **Apply** and **Save Configuration**.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave  
 NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP  
 SECURITY  
 Authentication  
 Access Control  
 WIRELESS  
 > **AP Configuration**  
 AP Installation  
 MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold  
 ADVANCED SERVICES  
 Redundancy  
 AirGroup  
 IP Mobility  
 Stateful Firewall

**Configuration > AP Group > Edit "default"**

Profiles	Profile Details
<ul style="list-style-type: none"> <li>Wireless LAN               <ul style="list-style-type: none"> <li>Virtual AP                   <ul style="list-style-type: none"> <li>cac</li> <li>VPSK</li> <li>spectralink-vap                       <ul style="list-style-type: none"> <li>AAA                           <ul style="list-style-type: none"> <li>spectralink-dot1x</li> </ul> </li> <li>802.11K                           <ul style="list-style-type: none"> <li>default</li> </ul> </li> <li>Hotspot 2.0                           <ul style="list-style-type: none"> <li>default</li> </ul> </li> <li>SSID                           <ul style="list-style-type: none"> <li>view</li> </ul> </li> <li>EDCA Parameters Station                           <ul style="list-style-type: none"> <li>AC_OFF</li> </ul> </li> <li>EDCA Parameters AP                           <ul style="list-style-type: none"> <li>AC_OFF</li> </ul> </li> <li>High-throughput SSID                           <ul style="list-style-type: none"> <li>default</li> </ul> </li> <li>802.11r                           <ul style="list-style-type: none"> <li>default</li> </ul> </li> <li>WMM Traffic Management</li> </ul> </li> <li>ADYS</li> <li>RF Management                   <ul style="list-style-type: none"> <li>AP</li> <li>QOS</li> <li>IDS</li> <li>Mesh</li> </ul> </li> </ul> </li> </ul> </li></ul>	<p>SSID Profile &gt; view <input type="button" value="Show Reference"/> <input type="button" value="Save As"/> <input type="button" value="Reset"/></p> <p>Basic Advanced</p> <p>SSID enable <input checked="" type="checkbox"/></p> <p>ESSID <input type="text" value="aruba-ap"/></p> <p>Encryption       <ul style="list-style-type: none"> <li><input type="checkbox"/> opensystem <input type="checkbox"/> static-wep</li> <li><input type="checkbox"/> dynamic-wep</li> <li><input type="checkbox"/> wpa-tkip <input type="checkbox"/> wpa-aes</li> <li><input type="checkbox"/> wpa-psk-tkip</li> <li><input type="checkbox"/> wpa-psk-aes <input checked="" type="checkbox"/> wpa2-aes</li> <li><input type="checkbox"/> wpa2-psk-aes</li> <li><input type="checkbox"/> wpa2-psk-tkip</li> <li><input type="checkbox"/> wpa2-tkip</li> </ul> </p> <p>DTIM Interval <input type="text" value="2"/> beacon periods</p> <p>802.11a Basic Rates       <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> 6 <input type="checkbox"/> 9 <input checked="" type="checkbox"/> 12 <input type="checkbox"/> 18 <input checked="" type="checkbox"/> 24</li> <li><input type="checkbox"/> 36 <input type="checkbox"/> 48 <input type="checkbox"/> 54</li> </ul> </p> <p>802.11a Transmit Rates       <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 12 <input checked="" type="checkbox"/> 18 <input checked="" type="checkbox"/> 24</li> <li><input checked="" type="checkbox"/> 36 <input checked="" type="checkbox"/> 48 <input checked="" type="checkbox"/> 54</li> </ul> </p> <p>802.11g Basic Rates       <ul style="list-style-type: none"> <li><input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 9 <input checked="" type="checkbox"/> 11</li> <li><input type="checkbox"/> 12 <input type="checkbox"/> 18 <input type="checkbox"/> 24 <input type="checkbox"/> 36</li> <li><input type="checkbox"/> 48 <input type="checkbox"/> 54</li> </ul> </p> <p>802.11g Transmit Rates       <ul style="list-style-type: none"> <li><input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 11</li> <li><input checked="" type="checkbox"/> 12 <input checked="" type="checkbox"/> 18 <input checked="" type="checkbox"/> 24 <input checked="" type="checkbox"/> 36</li> <li><input checked="" type="checkbox"/> 48 <input checked="" type="checkbox"/> 54</li> </ul> </p> <p>Station Ageout Time <input type="text" value="1000"/> sec</p> <p><input type="button" value="Apply"/></p>

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
AP  
Controller  
Campus WLAN  
Remote AP  
WIP  
AirWave  
NETWORK  
Controller  
VLANs  
Ports  
Uplink  
IP  
SECURITY  
Authentication  
Access Control  
WIRELESS  
AP Configuration  
AP Installation  
MANAGEMENT  
General  
Administration  
Certificates  
SNMP  
Logging  
Clock  
Guest Provisioning  
Captive Portal  
SMTP  
Bandwidth Calculator  
Threshold  
ADVANCED SERVICES  
Redundancy  
IP Mobility  
Stateful Firewall  
External Services  
VPN Services  
Wired Access  
All Profiles

**Configuration > AP Group > Edit "default"**

Profiles	Profile Details
Wireless LAN	Station Ageout Time 1000 sec
Virtual AP	Max Transmit Attempts 8
default	RTS Threshold 2333 bytes
data	Short Preamble <input checked="" type="checkbox"/>
VPSK2	Max Associations 64
VPEAP	Wireless Multimedia (WMM) <input checked="" type="checkbox"/>
AAA	Wireless Multimedia U-APSD (WMM-UAPSD) Powersave <input checked="" type="checkbox"/>
802.11K	WMM TSPEC Min Inactivity Interval 3600000 msec
Hotspot 2.0	Override DSCP mappings for WMM clients <input type="checkbox"/>
SSID	DSCP mapping for WMM voice AC 46
EDCA Parameters Station	DSCP mapping for WMM video AC 40
EDCA Parameters AP	DSCP mapping for WMM best-effort AC 0
High-throughput SSID	DSCP mapping for WMM background AC 0
802.11r	Multiple Tx Replay Counters <input type="checkbox"/>
WMM Traffic Management	Hide SSID <input type="checkbox"/>
VWEP	Deny_Broadcast Probes <input type="checkbox"/>
VPSK	Local Probe Request Threshold (dB) 0
RF Management	Disable Probe Retry <input checked="" type="checkbox"/>
AP	Battery Boost <input type="checkbox"/>
QOS	WEP Key 1 Retype:
IDS	WEP Key 2 Retype:
Mesh	

Commands [View Commands](#)

- Click **EDCA Parameters AP profile** and select the profile for the Spectralink phones from the dropdown.
- Change **ACM** field under the **Video and Voice AC** to **1** only if 87-Series handsets are not present in the network.



### Admin Tip: 87-Series, WMM-AC Incompatible

Spectralink 87-Series handsets have not yet implemented TSPEC control. They will not operate properly in a network with WMM-AC turned on.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave  
 NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP  
 SECURITY  
 Authentication  
 Access Control  
 WIRELESS  
 > **AP Configuration**  
 AP Installation  
 MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold  
 ADVANCED SERVICES  
 Redundancy

**Configuration > AP Group > Edit "default"**

Profiles	Profile Details																																							
<input type="checkbox"/> Wireless LAN <input type="checkbox"/> Virtual AP <input type="checkbox"/> cac <input type="checkbox"/> VPSK <input type="checkbox"/> spectralink-vap <input type="checkbox"/> AAA <input type="checkbox"/> 802.11K <input type="checkbox"/> Hotspot 2.0 <input type="checkbox"/> SSID <input type="checkbox"/> EDCA Parameters Station <input type="checkbox"/> EDCA Parameters AP <input type="checkbox"/> High-throughput SSID <input type="checkbox"/> 802.11r <input type="checkbox"/> WMM Traffic Management <input type="checkbox"/> ADYS <input type="checkbox"/> RF Management <input type="checkbox"/> AP <input type="checkbox"/> QoS <input type="checkbox"/> IDS <input type="checkbox"/> Mesh	<b>EDCA Parameters Station profile &gt; AC_OFF</b> Show Reference Save As Reset <table border="1"> <tr> <td rowspan="4">Best-effort</td> <td>aifsn</td> <td>3</td> </tr> <tr> <td>ecwmin</td> <td>4</td> </tr> <tr> <td>ecwmax</td> <td>10</td> </tr> <tr> <td>txop</td> <td>0</td> </tr> <tr> <td rowspan="4">Background</td> <td>aifsn</td> <td>7</td> </tr> <tr> <td>ecwmin</td> <td>4</td> </tr> <tr> <td>ecwmax</td> <td>10</td> </tr> <tr> <td>txop</td> <td>0</td> </tr> <tr> <td rowspan="4">Video</td> <td>aifsn</td> <td>2</td> </tr> <tr> <td>ecwmin</td> <td>3</td> </tr> <tr> <td>ecwmax</td> <td>4</td> </tr> <tr> <td>txop</td> <td>94</td> </tr> <tr> <td rowspan="4">Voice</td> <td>aifsn</td> <td>2</td> </tr> <tr> <td>ecwmin</td> <td>2</td> </tr> <tr> <td>ecwmax</td> <td>3</td> </tr> <tr> <td>txop</td> <td>47</td> </tr> <tr> <td></td> <td>acm</td> <td>0</td> </tr> </table>	Best-effort	aifsn	3	ecwmin	4	ecwmax	10	txop	0	Background	aifsn	7	ecwmin	4	ecwmax	10	txop	0	Video	aifsn	2	ecwmin	3	ecwmax	4	txop	94	Voice	aifsn	2	ecwmin	2	ecwmax	3	txop	47		acm	0
Best-effort	aifsn		3																																					
	ecwmin		4																																					
	ecwmax		10																																					
	txop	0																																						
Background	aifsn	7																																						
	ecwmin	4																																						
	ecwmax	10																																						
	txop	0																																						
Video	aifsn	2																																						
	ecwmin	3																																						
	ecwmax	4																																						
	txop	94																																						
Voice	aifsn	2																																						
	ecwmin	2																																						
	ecwmax	3																																						
	txop	47																																						
	acm	0																																						

Apply View Commands

Commands

**7** Click **EDCA Parameters Station** profile and select the profile for the Spectralink phones from the dropdown (Ex. Default If it is not desired to use the default EDCA Parameters profile, a new profile can be created, as shown in the example.)

- a** Change **ACM** field under **Video** and **Voice AC** to **1** only if 87-Series handsets are not present in the network.

**8** Click **Apply** and **Save Configuration**.

Dashboard | Monitoring | **Configuration** | Diagnostics | Maintenance | Save Configuration

WIZARDS

- AP
- Controller
- Campus WLAN
- Remote AP
- AirWave

NETWORK

- Controller
- VLANs
- Ports
- Cellular Profile
- IP

SECURITY

- Authentication
- Access Control

WIRELESS

- > **AP Configuration**
- AP Installation

MANAGEMENT

- General
- Administration
- Certificates
- SNMP
- Logging
- Clock
- Guest Provisioning
- Captive Portal
- SMTP
- Bandwidth Calculator
- Threshold

ADVANCED SERVICES

Configuration > AP Group > Edit "default"

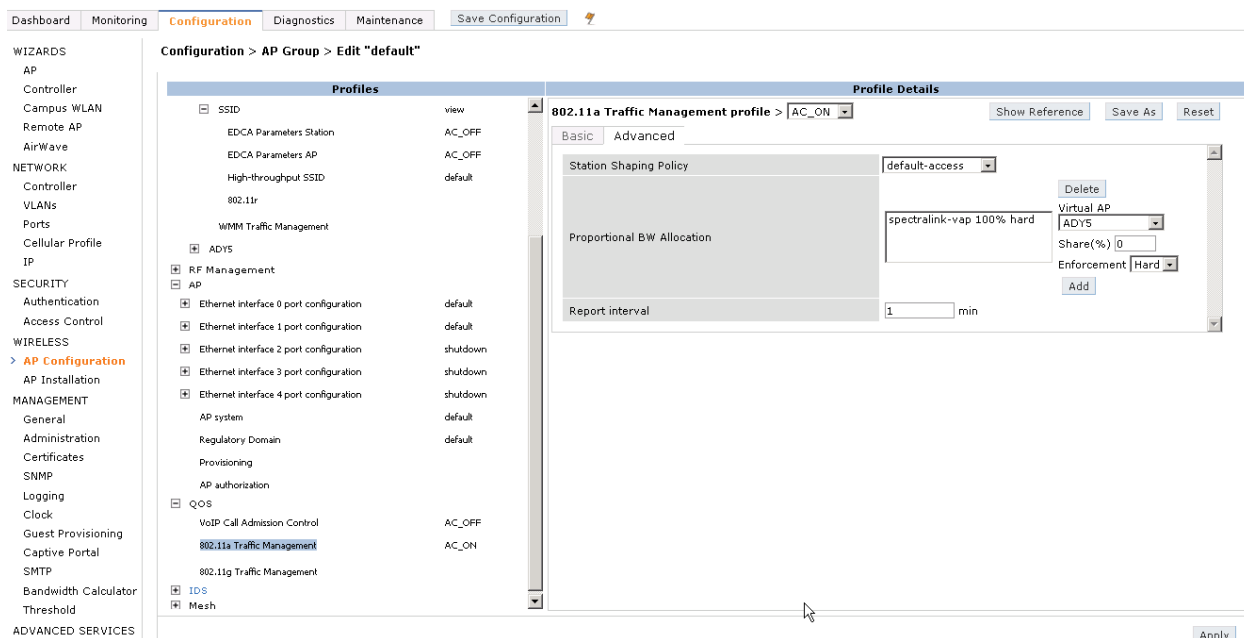
Profiles	Profile Details																														
<ul style="list-style-type: none"> <li>Wireless LAN               <ul style="list-style-type: none"> <li>Virtual AP                   <ul style="list-style-type: none"> <li>cac</li> <li>VPSK</li> <li>spectralink-vap</li> </ul> </li> <li>AAA                   <ul style="list-style-type: none"> <li>spectralink-dot1x</li> </ul> </li> <li>802.11K                   <ul style="list-style-type: none"> <li>default</li> </ul> </li> <li>Hotspot 2.0                   <ul style="list-style-type: none"> <li>default</li> </ul> </li> <li>SSID                   <ul style="list-style-type: none"> <li>view</li> </ul> </li> <li>EDCA Parameters Station                   <ul style="list-style-type: none"> <li>AC_OFF</li> </ul> </li> <li>EDCA Parameters AP                   <ul style="list-style-type: none"> <li>AC_OFF</li> </ul> </li> <li>High-throughput SSID                   <ul style="list-style-type: none"> <li>default</li> </ul> </li> <li>802.11r                   <ul style="list-style-type: none"> <li>default</li> </ul> </li> <li>WMM Traffic Management                   <ul style="list-style-type: none"> <li>ADFS</li> </ul> </li> <li>RF Management                   <ul style="list-style-type: none"> <li>AP</li> <li>QoS</li> <li>IDS</li> <li>Mesh</li> </ul> </li> </ul> </li> </ul>	<p>EDCA Parameters AP profile &gt; AC_OFF</p> <p>Show Reference Save As Reset</p> <table border="1"> <thead> <tr> <th>Profile</th> <th>aifsn</th> <th>ecwmin</th> <th>ecwmax</th> <th>txop</th> <th>acm</th> </tr> </thead> <tbody> <tr> <td>Best-effort</td> <td>3</td> <td>4</td> <td>6</td> <td>0</td> <td>0</td> </tr> <tr> <td>Background</td> <td>7</td> <td>4</td> <td>10</td> <td>0</td> <td>0</td> </tr> <tr> <td>Video</td> <td>1</td> <td>3</td> <td>4</td> <td>94</td> <td>0</td> </tr> <tr> <td>Voice</td> <td>1</td> <td>2</td> <td>3</td> <td>47</td> <td>0</td> </tr> </tbody> </table>	Profile	aifsn	ecwmin	ecwmax	txop	acm	Best-effort	3	4	6	0	0	Background	7	4	10	0	0	Video	1	3	4	94	0	Voice	1	2	3	47	0
Profile	aifsn	ecwmin	ecwmax	txop	acm																										
Best-effort	3	4	6	0	0																										
Background	7	4	10	0	0																										
Video	1	3	4	94	0																										
Voice	1	2	3	47	0																										

Apply

## Creating a Traffic Management Profile

- 1 Click **AP Configuration**.
- 2 Click **QoS**.
- 3 Click **802.11a Traffic Management profile**.
  - a On the right pane in the dropdown list **802.11a Traffic Management profile**, select **NEW** and enter a CaC profile name (Ex., AC\_ON).
  - b On the dropdown list under **Virtual AP**, select the virtual AP profile created above (in this example, spectralink-vap).
  - c Enter **100%** in the **Share(%)** box and click **Add** to allocate all of the tracked bandwidth to the voice virtual AP.
  - d Set the Enforcement to **Hard**.
  - e Change the **Report interval** to **1 min**.
  - f Click **Apply** and **Save Configuration**.
- 4 Click **802.11g Traffic Management profile** in the left hand side of the pane.
  - a Select **AC\_ON** (the profile created above) from the dropdown list **802.11g Traffic Management profile**.
  - b Click **Apply** and **Save Configuration**.





## Creating a VoIP CAC Profile

In the VoIP Call Admission Control Profile screen below, use the bandwidth from the table below that corresponds to the codec the phones on the network will be using. As described in *Spectralink 84-Series Wireless Telephone Administration Guide*, the 84-Series handsets support the codecs shown in the table below. If the configuration is not changed from the default described in the reference, the codec used will be the one shown first in the table that is supported by the other side of the call. The 84-Series handsets can be configured to add the optional codecs shown in the table. This feature is used when communicating with desksets with high definition audio.

The 8020/8030 phones support G.711 $\mu$ -law, G.711a-law and G.729 codecs but always ask for the largest bandwidth allocation, so only one entry is needed per radio band.

Choose the bandwidth from the table below that is the smallest number needed to support the type of phones or codecs expected so that the number of calls will be limited to what the AP can support.

### 8000 Series Phones

Codec	Radio	Bandwidth
All	5.0 GHz	1500
All	2.4 GHz	1100

## 84-Series handsets Default Codecs (in priority order)

<i>Codec</i>	<i>Radio</i>	<i>Bandwidth</i>
G.722	5.0 GHz	3200
G.722	2.4 GHz	2000
G.722.1 (32 kbps)	5.0 GHz	2000
G.722.1 (32 kbps)	2.4 GHz	1600
G.711Mu-law	5.0 GHz	3200
G.711Mu-law	2.4 GHz	2400
G.711A-law	5.0 GHz	3200
G.711A-law	2.4 GHz	2400
G.729AB	5.0 GHz	1200
G.729AB	2.4 GHz	1000

## 84-Series handsets Configurable Codecs

<i>Codec</i>	<i>Radio</i>	<i>Bandwidth</i>
G.722.1 (16 kbps)	5.0 GHz	1400
G.722.1 (16 kbps)	2.4 GHz	1000
G.722.1 (24 kbps)	5.0 GHz	1800
G.722.1 (24 kbps)	2.4 GHz	1400
L16.8 (128 kbps)	5.0 GHz	6000
L16.8 (128 kbps)	2.4 GHz	4700
L16.16 (256 kbps)	5.0 GHz	5800
L16.16 (256 kbps)	2.4 GHz	4400

- 1 Note: this command disables deep packet inspection for SIP and must be used from the cli for proper WMM Access Control (TSPEC) operation. No GUI equivalent is currently available:

```
(Aruba651)# configure terminal
```

```
(Aruba651)# voice alg-based-cac disable
```

- 2 Click **AP Configuration**.
- 3 Click **QoS**.
- 4 On the right pane, select **NEW** and enter a Cac profile name (Ex., 8400\_g).
- 5 Click **Apply**.
- 6 Click the newly created profile name
  - a Click **VoIP Call Admission Control Profile**.
  - b Check **VoIP Call Admission Control**, **Enable only WMM-AC CAC**, and **VoIP Bandwidth based CAC**.
  - c Enter the bandwidth from the table in the **VoIP Bandwidth Capacity (kbps)** as described above.
  - d Uncheck **VOIP TSPEC Enforcement**, **VoIP Send SIP 100 Trying**, and **VoIP Disconnect Extra Call**.
  - e Select **none** from the **VoIP Drop SIP...** dropdown lists.
  - f Click **Apply** and **Save Configuration**.

Dashboard | Monitoring | **Configuration** | Diagnostics | Maintenance | Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave

NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP

SECURITY  
 Authentication  
 Access Control

WIRELESS  
 > **AP Configuration**

MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold

ADVANCED SERVICES

**Configuration > AP Group > Edit "default"**

Profiles		Profile Details	
Wireless LAN		VoIP Call Admission Control profile > AC_ON	
Virtual AP		Show Reference Save As Reset	
+	cac	Basic Advanced	
+	VPSK		
+	spectralink-vap		
+	AAA	spectralink-dot1x	
+	802.11K	default	
+	Hotspot 2.0	default	
+	SSID	view	
	EDCA Parameters Station	AC_ON	
	EDCA Parameters AP	AC_ON	
	High-throughput SSID	default	
	802.11r		
	WMM Traffic Management		
+	ADYS		
+	RF Management		
+	AP		
+	QoS		
	VoIP Call Admission Control	AC_ON	
	802.11a Traffic Management	AC_ON	
	802.11g Traffic Management	AC_ON	
+	IDS		
+	Mesh		

VoIP Call Admission Control profile > AC\_ON

Basic Advanced

VoIP Call Admission Control	<input checked="" type="checkbox"/>
VoIP Bandwidth based CAC	<input checked="" type="checkbox"/>
VoIP Call Capacity	10
VoIP Bandwidth Capacity (kbps)	2000
VoIP Call Handoff Reservation	20 %
VoIP Send SIP 100 Trying	<input type="checkbox"/>
VoIP Disconnect Extra Call	<input type="checkbox"/>
VoIP TSPEC Enforcement	<input type="checkbox"/>
VoIP TSPEC Enforcement Period	1 sec
VoIP Drop SIP Invite and send status code (client)	none
VoIP Drop SIP Invite and send status code (server)	none

Apply

## Creating a High-Throughput SSID profile for an 802.11n-disabled network

- 1 Click **High-Throughput SSID Profile**.
- 2 Drop down on the right-pane and select **NEW**. Provide name (Ex., ht-disabled).
- 3 Modify the following
  - a Uncheck **High-Throughput enable**.
- 4 Click **Apply**.
- 5 Click **Save Configuration**.

Dashboard | Monitoring | **Configuration** | Diagnostics | Maintenance | Save Configuration

WIZARDS  
AP  
Controller  
Campus WLAN  
Remote AP  
AirWave

NETWORK  
Controller  
VLANs  
Ports  
Cellular Profile  
IP

SECURITY  
Authentication  
Access Control

WIRELESS  
AP Configuration  
AP Installation

MANAGEMENT  
General  
Administration  
Certificates  
SNMP  
Logging  
Clock  
Guest Provisioning  
Captive Portal  
SMTP  
Bandwidth Calculator  
Threshold

ADVANCED SERVICES  
Redundancy  
AirGroup  
IP Mobility  
Stateful Firewall  
External Services  
VPN Services  
Wired Access  
All Profiles

**Configuration > AP Group > Edit "default"**

Profiles	Profile Details																																																				
<ul style="list-style-type: none"> <li>Wireless LAN           <ul style="list-style-type: none"> <li>Virtual AP               <ul style="list-style-type: none"> <li>cac</li> <li>VPSK                   <ul style="list-style-type: none"> <li>AAA: spectralink-aaa</li> <li>802.11K: default</li> <li>Hotspot 2.0: default</li> <li>SSID: VPSK                       <ul style="list-style-type: none"> <li>EDCA Parameters Station: AC_OFF</li> <li>EDCA Parameters AP: AC_OFF</li> <li><b>High-throughput SSID: ht-disable</b></li> <li>802.11r</li> <li>WMM Traffic Management</li> </ul> </li> </ul> </li> </ul> </li> <li>spectralink-vap               <ul style="list-style-type: none"> <li>ADYS</li> <li>RF Management                   <ul style="list-style-type: none"> <li>AP                       <ul style="list-style-type: none"> <li>QOS</li> <li>IDS</li> <li>Mesh</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul>	<p><b>High-throughput SSID Profile &gt;</b> ht-disable <span>Show Reference</span> <span>Save As</span> <span>Reset</span></p> <p>Basic   <b>Advanced</b></p> <table border="1"> <tr><td>High throughput enable (SSID)</td><td><input type="checkbox"/></td></tr> <tr><td>40 MHz channel usage</td><td><input type="checkbox"/></td></tr> <tr><td>Very High throughput enable (SSID)</td><td><input type="checkbox"/></td></tr> <tr><td>80 MHz channel usage (VHT)</td><td><input type="checkbox"/></td></tr> <tr><td>BA AMSDU Enable</td><td><input type="checkbox"/></td></tr> <tr><td>Temporal Diversity Enable</td><td><input type="checkbox"/></td></tr> <tr><td>Legacy stations</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Low-density Parity Check</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Maximum number of spatial streams usable for STBC reception</td><td>1</td></tr> <tr><td>Maximum number of spatial streams usable for STBC transmission</td><td>1</td></tr> <tr><td>MPDU Aggregation</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Max received A-MPDU size</td><td>65535</td></tr> <tr><td>Max transmitted A-MPDU size</td><td>65535 bytes</td></tr> <tr><td>Min MPDU start spacing</td><td>0</td></tr> <tr><td>Short guard interval in 20 MHz mode</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Short guard interval in 40 MHz mode</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Short guard interval in 80 MHz mode</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Supported MCS set</td><td>0-23</td></tr> <tr><td>VHT - Supported MCS map</td><td>9 9 9 9</td></tr> <tr><td>VHT - Explicit Transmit Beamforming</td><td><input type="checkbox"/></td></tr> <tr><td>VHT - Transmit Beamforming Sounding Interval</td><td>25 msec</td></tr> <tr><td>Maximum VHT MPDU size</td><td>11454</td></tr> <tr><td>Maximum number of MSDUs in an A-MSDU on best-effort AC</td><td>10 MSDUs</td></tr> <tr><td>Maximum number of MSDUs in an A-MSDU on background AC</td><td>10 MSDUs</td></tr> <tr><td>Maximum number of MSDUs in an A-MSDU on video AC</td><td>3 MSDUs</td></tr> <tr><td>Maximum number of MSDUs in an A-MSDU on voice AC</td><td>3 MSDUs</td></tr> </table> <p><span>Apply</span></p>	High throughput enable (SSID)	<input type="checkbox"/>	40 MHz channel usage	<input type="checkbox"/>	Very High throughput enable (SSID)	<input type="checkbox"/>	80 MHz channel usage (VHT)	<input type="checkbox"/>	BA AMSDU Enable	<input type="checkbox"/>	Temporal Diversity Enable	<input type="checkbox"/>	Legacy stations	<input checked="" type="checkbox"/>	Low-density Parity Check	<input checked="" type="checkbox"/>	Maximum number of spatial streams usable for STBC reception	1	Maximum number of spatial streams usable for STBC transmission	1	MPDU Aggregation	<input checked="" type="checkbox"/>	Max received A-MPDU size	65535	Max transmitted A-MPDU size	65535 bytes	Min MPDU start spacing	0	Short guard interval in 20 MHz mode	<input checked="" type="checkbox"/>	Short guard interval in 40 MHz mode	<input checked="" type="checkbox"/>	Short guard interval in 80 MHz mode	<input checked="" type="checkbox"/>	Supported MCS set	0-23	VHT - Supported MCS map	9 9 9 9	VHT - Explicit Transmit Beamforming	<input type="checkbox"/>	VHT - Transmit Beamforming Sounding Interval	25 msec	Maximum VHT MPDU size	11454	Maximum number of MSDUs in an A-MSDU on best-effort AC	10 MSDUs	Maximum number of MSDUs in an A-MSDU on background AC	10 MSDUs	Maximum number of MSDUs in an A-MSDU on video AC	3 MSDUs	Maximum number of MSDUs in an A-MSDU on voice AC	3 MSDUs
High throughput enable (SSID)	<input type="checkbox"/>																																																				
40 MHz channel usage	<input type="checkbox"/>																																																				
Very High throughput enable (SSID)	<input type="checkbox"/>																																																				
80 MHz channel usage (VHT)	<input type="checkbox"/>																																																				
BA AMSDU Enable	<input type="checkbox"/>																																																				
Temporal Diversity Enable	<input type="checkbox"/>																																																				
Legacy stations	<input checked="" type="checkbox"/>																																																				
Low-density Parity Check	<input checked="" type="checkbox"/>																																																				
Maximum number of spatial streams usable for STBC reception	1																																																				
Maximum number of spatial streams usable for STBC transmission	1																																																				
MPDU Aggregation	<input checked="" type="checkbox"/>																																																				
Max received A-MPDU size	65535																																																				
Max transmitted A-MPDU size	65535 bytes																																																				
Min MPDU start spacing	0																																																				
Short guard interval in 20 MHz mode	<input checked="" type="checkbox"/>																																																				
Short guard interval in 40 MHz mode	<input checked="" type="checkbox"/>																																																				
Short guard interval in 80 MHz mode	<input checked="" type="checkbox"/>																																																				
Supported MCS set	0-23																																																				
VHT - Supported MCS map	9 9 9 9																																																				
VHT - Explicit Transmit Beamforming	<input type="checkbox"/>																																																				
VHT - Transmit Beamforming Sounding Interval	25 msec																																																				
Maximum VHT MPDU size	11454																																																				
Maximum number of MSDUs in an A-MSDU on best-effort AC	10 MSDUs																																																				
Maximum number of MSDUs in an A-MSDU on background AC	10 MSDUs																																																				
Maximum number of MSDUs in an A-MSDU on video AC	3 MSDUs																																																				
Maximum number of MSDUs in an A-MSDU on voice AC	3 MSDUs																																																				

Configuration Updated Successfully.

## Creating a High-Throughput SSID profile for an 802.11n-enabled network

- 1 Click **High-Throughput SSID Profile**.
- 2 On the right pane, click on the **Advanced** tab.
- 3 Drop down on the right-pane and select **NEW**. Provide name (Ex., ht-enable-80).
- 4 Modify the following
  - a Check **High-Throughput enable**.
  - b Check **40 MHz channel usage** or uncheck for 20 MHz usage.
  - c Check **Very High throughput enable (SSID)** and **80 MHz channel usage (VHT)** if available or uncheck not to use 80 MHz. Note: the AP must be power cycled for the 80 MHz setting to take effect.



### Admin Tip: Paired channel recommendation

40 MHz (paired) channels are not recommended by Aruba on the 2.4 GHz radio band.

- d Ensure that **Temporal Diversity Enable** is unchecked.
- e Uncheck **MPDU Aggregation**.



**Admin Tip: Disable A-MPDU on handset SSIDs**

The Spectralink handsets do not implement A-MPDU aggregation. They cause extra traffic by declining Block ACK requests. It eliminates extra traffic to disable A-MPDU traffic on SSIDs used for handset traffic.

- f Check Legacy Stations. Note: this is not necessary if there are no non-11n devices in the network. This must be checked if 8020/8030 phones are present.
- g Check Short guard interval in 20 MHz mode.
- h Check Short guard interval in 40 MHz mode.
- i For 12x and 13x AP's, set the **Maximum number of MSDUs in an A-MSDU on best-effort AC** and the **Maximum number of MSDU's in an A-MSDU on background AC** both to 10. For 11n AP's with model numbers smaller than 12x, set these values to 3.
- j Set the **Maximum number of MSDUs in an A-MSDU on video AC** and **Maximum number of MSDUs in an A-MSDU on voice AC** both to 3.



**Admin Tip: A-MSDU Aggregation Settings**

The AP-125 and AP-135 and newer AP's can process 10 packets per background and best effort aggregation. Older 11n AP's have better performance with a setting of 3 packets per background and best effort aggregation. Voice and video should remain with 3 packets per aggregation to avoid audible/visible latency issues.

- 5 Click **Apply**.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave  
 NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP  
 SECURITY  
 Authentication  
 Access Control  
 WIRELESS  
 > **AP Configuration**  
 AP Installation  
 MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold  
 ADVANCED SERVICES  
 Redundancy  
 AirGroup  
 IP Mobility  
 Stateful Firewall  
 External Services  
 VPN Services  
 Wired Access  
 All Profiles

**Configuration > AP Group > Edit "default"**

Profiles	Profile Details																																																				
<ul style="list-style-type: none"> <li>Wireless LAN               <ul style="list-style-type: none"> <li>Virtual AP                   <ul style="list-style-type: none"> <li>cac</li> <li>VPSK</li> <li>spectralink-vap</li> <li>AAA                       <ul style="list-style-type: none"> <li>spectralink-dot1x</li> <li>802.11K                           <ul style="list-style-type: none"> <li>default</li> <li>Hotspot 2.0                               <ul style="list-style-type: none"> <li>default</li> <li>SSID                                   <ul style="list-style-type: none"> <li>view</li> <li>EDCA Parameters Station                                       <ul style="list-style-type: none"> <li>AC_OFF</li> <li>EDCA Parameters AP   <ul style="list-style-type: none"> <li>AC_OFF</li> <li>High-throughput SSID   <ul style="list-style-type: none"> <li>ht_enable_80</li> <li>802.11r</li> <li>WMM Traffic Management</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> <li>ADYS</li> <li>RF Management                   <ul style="list-style-type: none"> <li>AP</li> <li>QOS</li> <li>IDS</li> <li>Mesh</li> </ul> </li> </ul> </li> </ul> </li></ul></li></ul>	<p><b>High-throughput SSID Profile &gt;</b> ht_enable_80 Show Reference Save As Reset</p> <p>Basic Advanced</p> <table border="1"> <tbody> <tr><td>High throughput enable (SSID)</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>40 MHz channel usage</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Very High throughput enable (SSID)</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>80 MHz channel usage (VHT)</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>BA AMSDU Enable</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Temporal Diversity Enable</td><td><input type="checkbox"/></td></tr> <tr><td>Legacy stations</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Low-density Parity Check</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Maximum number of spatial streams usable for STBC reception</td><td>1</td></tr> <tr><td>Maximum number of spatial streams usable for STBC transmission</td><td>1</td></tr> <tr><td>MPDU Aggregation</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Max received A-MPDU size</td><td>65535</td></tr> <tr><td>Max transmitted A-MPDU size</td><td>65535 bytes</td></tr> <tr><td>Min MPDU start spacing</td><td>0</td></tr> <tr><td>Short guard interval in 20 MHz mode</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Short guard interval in 40 MHz mode</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Short guard interval in 80 MHz mode</td><td><input type="checkbox"/></td></tr> <tr><td>Supported MCS set</td><td>0-23 &lt;-- &gt;</td></tr> <tr><td>VHT - Supported MCS map</td><td>9 9 9 9</td></tr> <tr><td>VHT - Explicit Transmit Beamforming</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>VHT - Transmit Beamforming Sounding Interval</td><td>25 msec</td></tr> <tr><td>Maximum VHT MPDU size</td><td>11454</td></tr> <tr><td>Maximum number of MSDUs in an A-MSDU on best-effort AC</td><td>10 MSDUs</td></tr> <tr><td>Maximum number of MSDUs in an A-MSDU on background AC</td><td>10 MSDUs</td></tr> <tr><td>Maximum number of MSDUs in an A-MSDU on video AC</td><td>3 MSDUs</td></tr> <tr><td>Maximum number of MSDUs in an A-MSDU on voice AC</td><td>3 MSDUs</td></tr> </tbody> </table>	High throughput enable (SSID)	<input checked="" type="checkbox"/>	40 MHz channel usage	<input checked="" type="checkbox"/>	Very High throughput enable (SSID)	<input checked="" type="checkbox"/>	80 MHz channel usage (VHT)	<input checked="" type="checkbox"/>	BA AMSDU Enable	<input checked="" type="checkbox"/>	Temporal Diversity Enable	<input type="checkbox"/>	Legacy stations	<input checked="" type="checkbox"/>	Low-density Parity Check	<input checked="" type="checkbox"/>	Maximum number of spatial streams usable for STBC reception	1	Maximum number of spatial streams usable for STBC transmission	1	MPDU Aggregation	<input checked="" type="checkbox"/>	Max received A-MPDU size	65535	Max transmitted A-MPDU size	65535 bytes	Min MPDU start spacing	0	Short guard interval in 20 MHz mode	<input checked="" type="checkbox"/>	Short guard interval in 40 MHz mode	<input checked="" type="checkbox"/>	Short guard interval in 80 MHz mode	<input type="checkbox"/>	Supported MCS set	0-23 <-- >	VHT - Supported MCS map	9 9 9 9	VHT - Explicit Transmit Beamforming	<input checked="" type="checkbox"/>	VHT - Transmit Beamforming Sounding Interval	25 msec	Maximum VHT MPDU size	11454	Maximum number of MSDUs in an A-MSDU on best-effort AC	10 MSDUs	Maximum number of MSDUs in an A-MSDU on background AC	10 MSDUs	Maximum number of MSDUs in an A-MSDU on video AC	3 MSDUs	Maximum number of MSDUs in an A-MSDU on voice AC	3 MSDUs
High throughput enable (SSID)	<input checked="" type="checkbox"/>																																																				
40 MHz channel usage	<input checked="" type="checkbox"/>																																																				
Very High throughput enable (SSID)	<input checked="" type="checkbox"/>																																																				
80 MHz channel usage (VHT)	<input checked="" type="checkbox"/>																																																				
BA AMSDU Enable	<input checked="" type="checkbox"/>																																																				
Temporal Diversity Enable	<input type="checkbox"/>																																																				
Legacy stations	<input checked="" type="checkbox"/>																																																				
Low-density Parity Check	<input checked="" type="checkbox"/>																																																				
Maximum number of spatial streams usable for STBC reception	1																																																				
Maximum number of spatial streams usable for STBC transmission	1																																																				
MPDU Aggregation	<input checked="" type="checkbox"/>																																																				
Max received A-MPDU size	65535																																																				
Max transmitted A-MPDU size	65535 bytes																																																				
Min MPDU start spacing	0																																																				
Short guard interval in 20 MHz mode	<input checked="" type="checkbox"/>																																																				
Short guard interval in 40 MHz mode	<input checked="" type="checkbox"/>																																																				
Short guard interval in 80 MHz mode	<input type="checkbox"/>																																																				
Supported MCS set	0-23 <-- >																																																				
VHT - Supported MCS map	9 9 9 9																																																				
VHT - Explicit Transmit Beamforming	<input checked="" type="checkbox"/>																																																				
VHT - Transmit Beamforming Sounding Interval	25 msec																																																				
Maximum VHT MPDU size	11454																																																				
Maximum number of MSDUs in an A-MSDU on best-effort AC	10 MSDUs																																																				
Maximum number of MSDUs in an A-MSDU on background AC	10 MSDUs																																																				
Maximum number of MSDUs in an A-MSDU on video AC	3 MSDUs																																																				
Maximum number of MSDUs in an A-MSDU on voice AC	3 MSDUs																																																				

6 Click Save Configuration.

## Assigning an AAA-profile

- 1 Click **AAA Profile** on the middle pane and select the AAA profile created for the voice devices (spectralink-aaa for non-enterprise security or spectralink-dot1x for enterprise security).
- 2 Click **Apply** and **Save Configuration**.

Dashboard
Monitoring
Configuration
Diagnostics
Maintenance
Save Configuration

WIZARDS
AP
Controller
Campus WLAN
Remote AP
AirWave
NETWORK
Controller
VLANs
Ports
Cellular Profile
IP
SECURITY
Authentication
Access Control
WIRELESS
AP Configuration
AP Installation
MANAGEMENT
General
Administration
Certificates
SNMP
Logging
Clock
Guest Provisioning
Captive Portal
SMTP
Bandwidth Calculator
Threshold
ADVANCED SERVICES
Redundancy
AirGroup
IP Mobility
Stateful Firewall
External Services
VPN Services
Wired Access
All Profiles

## Configuration > AP Group > Edit "default"

Profiles	Profile Details																																				
<div>Wireless LAN</div> <div>Virtual AP</div> <div> cac VPSK spectralink-vap </div> <div> <div>AAA</div> spectralink-dot1x </div> <div> <div>802.11K</div> default </div> <div> <div>Hotspot 2.0</div> default </div> <div> <div>SSID</div> view </div> <div> EDCA Parameters Station AC_OFF </div> <div> EDCA Parameters AP AC_OFF </div> <div> High-throughput SSID default </div> <div> 802.11r </div> <div> WMM Traffic Management </div> <div> <div>ADYS</div> </div> <div> <div>RF Management</div> </div> <div> <div>AP</div> </div> <div> <div>QOS</div> </div> <div> <div>IDS</div> </div> <div> <div>Mesh</div> </div>	<div> <div>AAA Profile &gt;</div> spectralink-dot1x <div>Show Reference</div> </div> <table> <tr> <td>Initial role</td> <td>logon</td> </tr> <tr> <td>MAC Authentication Default Role</td> <td>guest</td> </tr> <tr> <td>802.1X Authentication Default Role</td> <td>guest</td> </tr> <tr> <td>L2 Authentication Fail Through</td> <td><input type="checkbox"/></td> </tr> <tr> <td>User idle timeout</td> <td> <input type="checkbox"/> Enable seconds </td> </tr> <tr> <td>RADIUS Interim Accounting</td> <td><input type="checkbox"/></td> </tr> <tr> <td>User derivation rules</td> <td>spectralink-derivation</td> </tr> <tr> <td>Wired to Wireless Roaming</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>SIP authentication role</td> <td>--NONE--</td> </tr> <tr> <td>Device Type Classification</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Enforce DHCP</td> <td><input type="checkbox"/></td> </tr> <tr> <td>MAC Authentication Profile</td> <td></td> </tr> <tr> <td>MAC Authentication Server Group</td> <td>default</td> </tr> <tr> <td>802.1X Authentication Profile</td> <td>spectralink-802.1x</td> </tr> <tr> <td>802.1X Authentication Server Group</td> <td>RADIUS</td> </tr> <tr> <td>RADIUS Accounting Server Group</td> <td></td> </tr> <tr> <td>XML API server</td> <td></td> </tr> <tr> <td>RFC 3576 server</td> <td></td> </tr> </table>	Initial role	logon	MAC Authentication Default Role	guest	802.1X Authentication Default Role	guest	L2 Authentication Fail Through	<input type="checkbox"/>	User idle timeout	<input type="checkbox"/> Enable seconds	RADIUS Interim Accounting	<input type="checkbox"/>	User derivation rules	spectralink-derivation	Wired to Wireless Roaming	<input checked="" type="checkbox"/>	SIP authentication role	--NONE--	Device Type Classification	<input checked="" type="checkbox"/>	Enforce DHCP	<input type="checkbox"/>	MAC Authentication Profile		MAC Authentication Server Group	default	802.1X Authentication Profile	spectralink-802.1x	802.1X Authentication Server Group	RADIUS	RADIUS Accounting Server Group		XML API server		RFC 3576 server	
Initial role	logon																																				
MAC Authentication Default Role	guest																																				
802.1X Authentication Default Role	guest																																				
L2 Authentication Fail Through	<input type="checkbox"/>																																				
User idle timeout	<input type="checkbox"/> Enable seconds																																				
RADIUS Interim Accounting	<input type="checkbox"/>																																				
User derivation rules	spectralink-derivation																																				
Wired to Wireless Roaming	<input checked="" type="checkbox"/>																																				
SIP authentication role	--NONE--																																				
Device Type Classification	<input checked="" type="checkbox"/>																																				
Enforce DHCP	<input type="checkbox"/>																																				
MAC Authentication Profile																																					
MAC Authentication Server Group	default																																				
802.1X Authentication Profile	spectralink-802.1x																																				
802.1X Authentication Server Group	RADIUS																																				
RADIUS Accounting Server Group																																					
XML API server																																					
RFC 3576 server																																					

## Assigning a 5 GHz Radio-profile

- 1 Click **RF Management** under the **Virtual AP**.
- 2 Click **802.11a radio-profile**.
- 3 Click the **Advanced** tab.
  - a Click **Radio enable** to turn the 802.11a radio on.
  - b In the default profile on the right-pane, enter a 5 GHz channel.
  - c Clear or set the High throughput enable (radio) according to whether the radio is 802.11n-enabled mode or not.
  - d Choose a **Transmit EIRP** chosen to support the site survey plan and the maximum mandatory data rate as described immediately below.





### Admin Tip: Transmit Power

For setting up the **Transmit Power**, please consult your facility's RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. Spectralink Wireless Telephones require the following minimum dBm reading to support the corresponding **Mandatory** data rate setting in the access point.

<i>802.11 Radio Standard</i>	<i>Minimum Available Signal Strength (RSSI)</i>	<i>Maximum "Mandatory" Data Rate</i>
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s



### Web Info: RF Deployment reference

For additional details on RF deployment please see the *Deploying Enterprise-Grade Wi-Fi Telephony* White Paper.

- e If DFS channels are to be used (channels shared with radar applications)
    - a. Click **Advertise 802.11d and 802.11h Capabilities**
    - b. Click **Enable CSA**.
    - c. Set **CSA Count** to 4.
  - f Ensure that **Spectrum Load Balancing** is unchecked.
  - g Ensure that **Advertised regulatory max EIRP** is 0.
- 4 Click **Apply**.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave

NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP

SECURITY  
 Authentication  
 Access Control

WIRELESS  
 > **AP Configuration**  
 AP Installation

MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold

ADVANCED SERVICES  
 Redundancy  
 AirGroup  
 IP Mobility  
 Stateful Firewall  
 External Services  
 VPN Services  
 Wired Access  
 All Profiles

**Configuration > AP Group > Edit "default"**

Profiles	Profile Details
<input type="checkbox"/> Wireless LAN <input type="checkbox"/> Virtual AP <input type="checkbox"/> RF Management <input checked="" type="checkbox"/> <b>802.11a radio</b> default Adaptive Radio Management (ARM) default High-throughput Radio default-a AM Scanning default <input type="checkbox"/> 802.11g radio default RF Optimization default RF Event Thresholds default <input checked="" type="checkbox"/> <b>AP</b> <input checked="" type="checkbox"/> QOS <input checked="" type="checkbox"/> IDS <input checked="" type="checkbox"/> Mesh	<b>802.11a radio profile &gt; default</b> Show Reference Save As Reset Basic Advanced Radio enable <input checked="" type="checkbox"/> Mode ap-mode High throughput enable (radio) <input checked="" type="checkbox"/> Very high throughput enable (radio) <input checked="" type="checkbox"/> Channel 149 Channel Width: <input type="radio"/> 20MHz <input type="radio"/> 40MHz <input checked="" type="radio"/> 80MHz Transmit EIRP 3 Non-Wi-Fi Interference Immunity 2 Enable CSA <input checked="" type="checkbox"/> CSA Count 4 Advertise 802.11d and 802.11h Capabilities <input checked="" type="checkbox"/> Spectrum Load Balancing <input type="checkbox"/> Beacon Period 100 msec Beacon Regulate <input type="checkbox"/> Advertized regulatory max EIRP 0 ARM/WIDS Override OFF Reduce Cell Size (Rx Sensitivity) 0 dB Management Frame Throttle interval 1 sec Management Frame Throttle Limit 20 Maximum Distance 0 meters RX Sensitivity Threshold 0 dB RX Sensitivity Tuning Based Channel Reuse disable

Commands Apply View Commands

- 5 Click **Adaptive Radio Management (ARM)** profile and then the **Advanced** tab.
- 6 Enter the settings as follows
  - a Ensure that **Assignment** is set to **disable** or **maintain**.
  - b Set **Allowed bands for 40MHz channels** to **a-only**.
  - c Check **Client Aware**.
  - d Ensure that **Active Scan** is not checked.
  - e Ensure that **ARM Over the Air Updates**, **Scanning**, **Multi Band Scan**, **VoIP Aware Scan**, **Power Save Aware Scan**, and **Video Aware Scan** are checked.
  - f Ensure that **Client Match** NOT checked.
- 7 Click **Apply** and **Save Configuration**.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave  
 NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP  
 SECURITY  
 Authentication  
 Access Control  
 WIRELESS  
 > **AP Configuration**  
 AP Installation  
 MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold  
 ADVANCED SERVICES  
 Redundancy  
 AirGroup  
 IP Mobility  
 Stateful Firewall  
 External Services  
 VPN Services  
 Wired Access  
 All Profiles

**Configuration > AP Group > Edit "default"**

Profiles		Profile Details	
<input type="checkbox"/> Wireless LAN			
<input checked="" type="checkbox"/> Virtual AP			
<input type="checkbox"/> RF Management			
<input checked="" type="checkbox"/> 802.11a radio	default		
<b>Adaptive Radio Management (ARM)</b>	default		
High-throughput Radio	default-a		
AM Scanning	default		
<input checked="" type="checkbox"/> 802.11g radio	default		
RF Optimization	default		
RF Event Thresholds	default		
<input checked="" type="checkbox"/> AP			
<input checked="" type="checkbox"/> QOS			
<input checked="" type="checkbox"/> IDS			
<input checked="" type="checkbox"/> Mesh			

Profile Details	
Basic	Advanced
Assignment	disable
Allowed bands for 40MHz channels	a-only
80MHz support	<input checked="" type="checkbox"/>
Client Aware	<input checked="" type="checkbox"/>
Max Tx EIRP	127
Min Tx EIRP	9
Rogue AP Aware	<input type="checkbox"/>
Active Scan	<input type="checkbox"/>
ARM Over the Air Updates	<input checked="" type="checkbox"/>
Scanning	<input checked="" type="checkbox"/>
Multi Band Scan	<input checked="" type="checkbox"/>
VoIP Aware Scan	<input checked="" type="checkbox"/>
Power Save Aware Scan	<input checked="" type="checkbox"/>
Video Aware Scan	<input checked="" type="checkbox"/>
Ideal Coverage Index	10
Acceptable Coverage Index	4
Free Channel Index	25
Backoff Time	240 sec
Error Rate Threshold	50 %
Error Rate Wait Time	30 sec
Channel Quality Aware Arm	<input type="checkbox"/>
Channel Quality Threshold	70 %
Channel Quality Wait Time	120 sec
Minimum Scan Time	8
Load aware Scan Threshold	1250000 Bps
Mode Aware Arm	<input type="checkbox"/>
Scan Mode	all-reg-domain
Cellular handoff assist	<input type="checkbox"/>
Client Match	<input type="checkbox"/>

Apply

**8** Click **High-Throughput Radio profile** (default-a).

**a** Ensure that CSD override is checked.

**b** Click **Apply** and **Save Configuration**.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave

NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP

SECURITY  
 Authentication  
 Access Control

WIRELESS  
 > **AP Configuration**  
 AP Installation

MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold

ADVANCED SERVICES  
 Redundancy  
 AirGroup  
 IP Mobility  
 Stateful Firewall  
 External Services  
 VPN Services  
 Wired Access  
 All Profiles

**Configuration > AP Group > Edit "default"**

Profiles	Profile Details
<ul style="list-style-type: none"> <li>Wireless LAN               <ul style="list-style-type: none"> <li>Virtual AP</li> <li>RF Management                   <ul style="list-style-type: none"> <li>802.11a radio default</li> <li>Adaptive Radio Management (ARM) default</li> <li><b>High-throughput Radio</b> default-a</li> <li>AM Scanning default</li> </ul> </li> <li>802.11g radio default</li> <li>RF Optimization default</li> <li>RF Event Thresholds default</li> </ul> </li> <li>AP</li> <li>QOS</li> <li>IDS</li> <li>Mesh</li> </ul>	<p>High-throughput Radio Profile &gt; default-a <span>Show Reference</span> <span>Save As</span> <span>Reset</span></p> <p>Basic Advanced</p> <p>40 MHz intolerance <input type="checkbox"/></p> <p>Honor 40 MHz intolerance <input type="checkbox"/></p> <p>CSD override <input checked="" type="checkbox"/></p>

Apply

## Assigning a 2.4 GHz Radio-profile

- 1 Click **802.11g radio-profile**.
- 2 Click the **Advanced** tab.
  - a Click **Radio enable** to turn the 802.11g radio on.
  - b In the default profile on the right-pane, enter a 2.4 GHz channel.
  - c Clear or set the High throughput enable (radio) according to whether the radio is 802.11n-enabled mode or not. Use only a 20 MHz width.
  - d Choose a Transmit EIRP chosen to support the site survey plan and the maximum mandatory data rate as described immediately below.

**Admin Tip: Transmit Power**

For setting up the **Transmit Power**, please consult your facility's RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. Spectralink Wireless Telephones require the following minimum dBm reading to support the corresponding **Mandatory** data rate setting in the access point.

<i>802.11 Radio Standard</i>	<i>Minimum Available Signal Strength (RSSI)</i>	<i>Maximum "Mandatory" Data Rate</i>
802.11b	-65 dBm	11 Mb/s
802.11g	-67 dBm	6 Mb/s
802.11g	-47 dBm	54 Mb/s

**Web Info: RF Deployment reference**

For additional details on RF deployment please see the *Deploying Enterprise-Grade Wi-Fi Telephony* White Paper.

Dashboard | Monitoring | **Configuration** | Diagnostics | Maintenance | Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave

NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP

SECURITY  
 Authentication  
 Access Control

WIRELESS  
 > **AP Configuration**  
 AP Installation

MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold

ADVANCED SERVICES  
 Redundancy  
 AirGroup  
 IP Mobility  
 Stateful Firewall  
 External Services  
 VPN Services  
 Wired Access  
 All Profiles

**Configuration > AP Group > Edit "default"**

Profiles	Profile Details
<ul style="list-style-type: none"> <li>Wireless LAN               <ul style="list-style-type: none"> <li>Virtual AP</li> <li>RF Management                   <ul style="list-style-type: none"> <li>802.11a radio: default</li> <li>Adaptive Radio Management (ARM): default</li> <li>High-throughput Radio: default-a</li> <li>AM Scanning: default</li> <li><b>802.11g radio: default</b></li> <li>Adaptive Radio Management (ARM): default</li> <li>High-throughput Radio: default-g</li> <li>AM Scanning: default</li> <li>RF Optimization: default</li> <li>RF Event Thresholds: default</li> </ul> </li> </ul> </li> <li>AP</li> <li>QoS</li> <li>IDS</li> <li>Mesh</li> </ul>	<p>802.11g radio profile &gt; default <span>Show Reference</span> <span>Save As</span> <span>Reset</span></p> <p>Basic <span>Advanced</span></p> <p><b>General</b></p> <p>Radio enable <input checked="" type="checkbox"/></p> <p>Mode: ap-mode</p> <p>High throughput enable (radio) <input checked="" type="checkbox"/></p> <p>TurboQAM rates enable (radio) <input type="checkbox"/></p> <p>Channel: 6 <span>Channel Width: <input checked="" type="radio"/> 20MHz <input type="radio"/> 40MHz</span></p> <p>Non-Wi-Fi Interference Immunity: 2</p> <p><span>Apply</span></p>

- 3 Click **Adaptive Radio Management (ARM) profile** and then the **Advanced** tab.
- 4 Enter the settings as follows
  - a Ensure that **Assignment** is set to **disable** or **maintain**.
  - b Set **Allowed bands for 40MHz channels** to **a-only**.
  - c Check **Client Aware**.
  - d Ensure that **Active Scan** is not checked.
  - e Ensure that **ARM Over the Air Updates, Scanning, Multi Band Scan, VoIP Aware Scan, Power Save Aware Scan, and Video Aware Scan** are checked.
  - f Ensure that **Client Match** is NOT checked.

Dashboard | Monitoring | **Configuration** | Diagnostics | Maintenance | Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave  
 NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP  
 SECURITY  
 Authentication  
 Access Control  
 WIRELESS  
 > **AP Configuration**  
 AP Installation  
 MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold  
 ADVANCED SERVICES  
 Redundancy  
 AirGroup  
 IP Mobility  
 Stateful Firewall  
 External Services  
 VPN Services  
 Wired Access  
 All Profiles

**Configuration > AP Group > Edit "default"**

Profiles		Profile Details	
<input type="checkbox"/> Wireless LAN		Basic	Advanced
<input type="checkbox"/> Virtual AP			
<input type="checkbox"/> RF Management			
<input type="checkbox"/> 802.11a radio	default		
Adaptive Radio Management (ARM)	default		
High-throughput Radio	default-a		
AM Scanning	default		
<input type="checkbox"/> 802.11g radio	default		
Adaptive Radio Management (ARM)	default		
High-throughput Radio	default-g		
AM Scanning	default		
RF Optimization	default		
RF Event Thresholds	default		
<input type="checkbox"/> AP			
<input type="checkbox"/> QOS			
<input type="checkbox"/> IDS			
<input type="checkbox"/> Mesh			

Assignment: disable  
 Allowed bands for 40MHz channels: a-only  
 80MHz support: ☒  
 Client Aware: ☒  
 Max Tx EIRP: 127  
 Min Tx EIRP: 9  
 Rogue AP Aware: ☐  
 Active Scan: ☐  
 ARM Over the Air Updates: ☒  
 Scanning: ☒  
 Multi Band Scan: ☒  
 VoIP Aware Scan: ☒  
 Power Save Aware Scan: ☒  
 Video Aware Scan: ☒  
 Ideal Coverage Index: 10  
 Acceptable Coverage Index: 4  
 Free Channel Index: 25  
 Backoff Time: 240 sec  
 Error Rate Threshold: 50 %  
 Error Rate Wait Time: 30 sec  
 Channel Quality Aware Arm: ☐  
 Channel Quality Threshold: 70 %  
 Channel Quality Wait Time: 120 sec  
 Minimum Scan Time: 8  
 Load aware Scan Threshold: 1250000 Bps  
 Mode Aware Arm: ☐  
 Scan Mode: all-reg-domain  
 Cellular handoff assist: ☐  
 Client Match: ☐

Apply

- 5 Click **High-Throughput Radio profile (default-g)** and then the **Advanced** tab.
  - a Check **CSD override**.
  - b Click **Apply**.
- 6 Click **Save Configuration**.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave

NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP

SECURITY  
 Authentication  
 Access Control

WIRELESS  
 > **AP Configuration**  
 AP Installation

MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold

ADVANCED SERVICES  
 Redundancy  
 AirGroup  
 IP Mobility  
 Stateful Firewall  
 External Services  
 VPN Services  
 Wired Access  
 All Profiles

**Configuration > AP Group > Edit "default"**

Profiles		Profile Details	
<input type="checkbox"/> Wireless LAN		<b>High-throughput Radio Profile &gt;</b> default-g <a href="#">Show Reference</a> <a href="#">Save As</a> <a href="#">Reset</a>	
<input type="checkbox"/> Virtual AP		Basic Advanced	
<input type="checkbox"/> RF Management		<div> <div>40 MHz intolerance</div> <div>Honor 40 MHz intolerance</div> <div>CSD override</div> </div>	
<input type="checkbox"/> 802.11a radio	default		
Adaptive Radio Management (ARM)	default		
High-throughput Radio	default-a		
AM Scanning	default		
<input type="checkbox"/> 802.11g radio	default		
Adaptive Radio Management (ARM)	default		
High-throughput Radio	default-g		
AM Scanning	default		
RF Optimization	default		
RF Event Thresholds	default		
<input type="checkbox"/> AP			
<input type="checkbox"/> QOS			
<input type="checkbox"/> IDS			
<input type="checkbox"/> Mesh			

Apply

At this point, the Mobility Controller is ready to provide Spectralink voice services.



# Section 2: Configuration for SVP Operation with Spectralink 8020/8030 Handsets

## Introduction

Spectralink 8020/8030 handsets can be configured for SVP QoS from the WLAN Settings menu using the Custom selection. Spectralink 84-Series and 87-Series handsets do not support SVP.

## Command, Comment, and Screen Text Key

In the sections below you will find commands, comments, prompts, system responses, or **other** screen-displayed information involved in the configuration process. This key explains the text styles and symbols used to denote them.

<b><i>Text Style</i></b>	<b><i>Denotes:</i></b>
<b>xxxxxxx</b>	Typed command
<b>&lt;xxxxxxx&gt;</b>	Encryption key, domain name or other information specific to your system that needs to be entered
<b>(xxxxxxx)</b>	Comment about a command or set of commands
<b>xxxxxxx</b>	Prompt, system response or other displayed information

## Connecting to the Mobility Controller

### Via console

Using a standard RS-232 cable, connect the Aruba mobility controller to the serial port of a terminal or PC.

Run a terminal emulation program (such as HyperTerminal™) or use a VT-100 terminal with the following configuration:

Bits per second:	9600
Data bits:	8
Parity:	None
Stop bits:	1
Flow control:	None

Use this mode of connection during the initialization phase of the controller to configure login credentials.

- 1 Press **Enter** to display the Aruba mobility controller login screen.
- 2 Enter the default login: **admin** and the default password: **admin**. These are case sensitive.
- 3 Enter **enable** and the default password: **enable** to get into the command mode.

### Via the CLI

By default, only SSH (Secure Shell) access to the switch (mobility controller) is permitted.

- 1 From a management system that has network connectivity to the switch, connect to the switch using SSH

```
ssh admin@<switch IP address>
```

- 2 Enter the admin password at the password prompt.

```
Type enable at the > prompt to enter the enable mode.
```

- 3 Type the enable password when prompted for a password.

### Via the Web interface (WebUI)

Once the connectivity to the switch is verified, open a Web browser and enter the switch's IP address in the navigator bar.

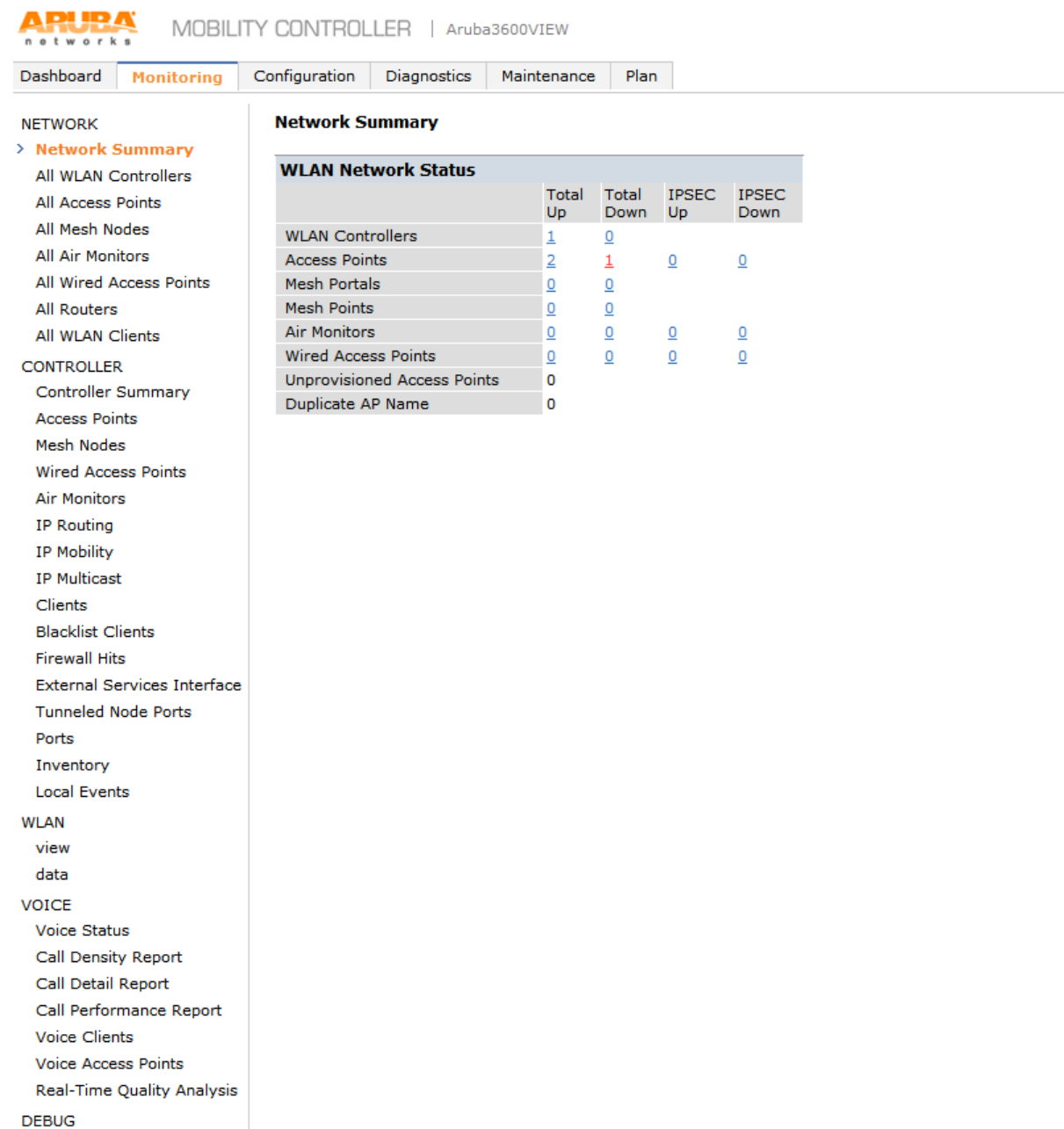
The switch can be accessed using http at

**http://<switch IP Address>**

or https at

**https://<switch IP Address>:4343.**

The user is prompted with the username and password configured (in the example above, the username/password configured is **admin/admin**). On successful login the following **Monitoring** screen is displayed:



**ARUBA** networks | MOBILITY CONTROLLER | Aruba3600VIEW

Dashboard **Monitoring** Configuration Diagnostics Maintenance Plan

**NETWORK**

- > **Network Summary**
  - All WLAN Controllers
  - All Access Points
  - All Mesh Nodes
  - All Air Monitors
  - All Wired Access Points
  - All Routers
  - All WLAN Clients

**CONTROLLER**

- Controller Summary
- Access Points
- Mesh Nodes
- Wired Access Points
- Air Monitors
- IP Routing
- IP Mobility
- IP Multicast
- Clients
- Blacklist Clients
- Firewall Hits
- External Services Interface
- Tunneled Node Ports
- Ports
- Inventory
- Local Events

**WLAN**

- view
- data

**VOICE**

- Voice Status
- Call Density Report
- Call Detail Report
- Call Performance Report
- Voice Clients
- Voice Access Points
- Real-Time Quality Analysis

**DEBUG**

**Network Summary**

WLAN Network Status				
	Total Up	Total Down	IPSEC Up	IPSEC Down
WLAN Controllers	1	0		
Access Points	2	1	0	0
Mesh Portals	0	0		
Mesh Points	0	0		
Air Monitors	0	0	0	0
Wired Access Points	0	0	0	0
Unprovisioned Access Points	0			
Duplicate AP Name	0			

## Initializing the Controller

When powered up, the controller will present the following screen on the serial console. Please fill in basic network details when prompted.

```
<<<<< Welcome to Aruba Networks - Aruba A3600 >>>>>

Performing CompactFlash fast test... Checking for file system...
Passed.
Reboot Cause: User reboot.
Restoring the database...done.
Generating SSH Keys.....done.
Reading configuration from factory-default.cfg

***** Welcome to the Aruba651 setup dialog *****
This dialog will help you to set the basic configuration for the switch.
These settings, except for the Country Code, can later be changed from the
Command Line Interface or Graphical User Interface.

Commands: <Enter> Submit input or use [default value], <ctrl-I> Help
<ctrl-B> Back, <ctrl-F> Forward, <ctrl-A> Line begin, <ctrl-E> Line end
<ctrl-D> Delete, <BackSpace> Delete back, <ctrl-K> Delete to end of line
<ctrl-P> Previous question <ctrl-X> Restart beginning

Enter System name [Aruba651]
Enter VLAN 1 interface IP address [172.16.0.254]: <Controller IP>
Enter VLAN 1 interface subnet mask [255.255.255.0]: <Subnet Mask>
Enter IP Default gateway [none]: <Default GW IP address>
Enter Switch Role, (master|local) [master]
This controller is restricted to Country code US for United States, please
confirm (yes|no)? : yes
Enter Time Zone [PST-8:0]
Enter Time in GMT [15:39:55]
Enter Date (MM/DD/YYYY) [4/21/2009]
Enter Password for admin login (up to 32 chars): *****
Re-type Password for admin login: *****
Enter Password for enable mode (up to 15 chars): *****
```

Re-type Password for enable mode: \*\*\*\*\*

Do you wish to shutdown all the ports (yes|no)? [no]: no

Current choices are

System name: Aruba651

VLAN 1 interface IP address: <IP Address>

VLAN 1 interface subnet mask: <Subnet Mask>

IP Default gateway: <Default Gateway>

Switch Role: master

Time Zone: PST-8:0

Ports shutdown: no

If you accept the changes the switch will restart!

Type <ctrl-P> to go back and change answer for any question

Do you wish to accept the changes (yes|no): yes

Creating configuration... Done.

System will now restart!

## *Licensing the Controller*

In order to avail of the stateful firewall features on the Aruba WLAN for identification of prioritization of Spectralink voice traffic, it is essential to have the Policy Enforcement Firewall Module and the Voice Services Module. Please contact your local Aruba representative. License Management can be easily done on the License Wizard of the WebUI.

You will need

- The Serial Number of the Mobility Controller.
- The License Certificate Number of the service to be activated (Please contact your local Aruba team).

Obtain the license Key from: <https://licensing.arubanetworks.com>

### **On the WebUI**

- 1 Click the **Configuration** tab.
- 2 On the left pane, click **Licenses**.
- 3 Click **Add** by **Add New License Key** (scroll down to see option).
- 4 Enter the license Key in the space provided and click **OK**.
- 5 Repeat 3 and 4 for all the licenses desired.
- 6 Click **Save Configuration**.
- 7 Verify that the licenses show up on the table in the same screen.
- 8 Centralized Licensing and a license server may also be used. See the Aruba User's Guide for details.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
AP  
Controller  
Campus WLAN  
Remote AP  
AirWave  
NETWORK  
VLANs  
Ports  
Cellular Profile  
IP  
SECURITY  
Authentication  
Access Control  
WIRELESS  
AP Configuration  
AP Installation  
MANAGEMENT  
General  
Administration  
Certificates  
SNMP  
Logging  
Clock  
Guest Provisioning  
Captive Portal  
SMTP  
Bandwidth Calculator  
Threshold  
ADVANCED SERVICES  
Redundancy  
AirGroup  
IP Mobility  
Stateful Firewall  
External Services  
VPN Services  
Wired Access  
All Profiles

**Network > Controller > License Management**

System Settings Control Plane Security Cluster Settings **Licenses** Centralized Licenses Sync whitelist service

### License Information

Service Status and Current Limits		To obtain license keys via the web:
Access Points	32	<b>Licensing Web Site:</b> <a href="https://licensing.arubanetworks.com">https://licensing.arubanetworks.com</a> <b>You will need the following:</b> <ul style="list-style-type: none"> <li>The serial number of the switch or supervisory module</li> <li>The license certificate number of the service you wish to activate</li> </ul>
Remote Access Points	32	
Outdoor Mesh Access Points	512	<ul style="list-style-type: none"> <li>The serial number to use for this switch is: AC0002304</li> </ul>
RF Protect	0	
Voice Service Module	Unlimited	
VPN Server Module	8192	
xSec Module	0	
Indoor Mesh Access Points	512	
Next Generation Policy Enforcement Firewall Module	32	
Advanced Cryptography	0	
Service provider AP	0	
RF Protect	DISABLED	
Policy Enforcement Firewall	ENABLED	
Remote APs	ENABLED	
External Services Interface	ENABLED	
Client Integrity Module	ENABLED	
VPN Server	ENABLED	
xSec Module	DISABLED	
MMC AP	DISABLED	
Netgear AP	DISABLED	
Voice Services Module	ENABLED	
Mesh Point APs	ENABLED	
AP Developers Module	DISABLED	
Internal Test Functions	DISABLED	
Public Access	DISABLED	
Policy Enforcement Firewall for VPN users	DISABLED	
Advanced Cryptography	DISABLED	
Service Provider Access Point	DISABLED	
Maritime Regulatory Domain	DISABLED	

AP Licenses		User License Usage	
AP Licenses	32	License Limit	8192
PEF Licenses	32	License Usage	0
Overall AP License Limit	32	License Available	8192
		License Exceeded	0

AP Usage	
Active CAPs	1
Standby CAPs	0
RAPs	0
Remote-node APs	0
Tunneled nodes	0
Total APs	1

Remaining AP Capacity	
CAPs	31
RAPs	31

License Exceeded	
License Exceeded	0

xSec License Usage	
License Limit	0
License Usage	0
License Exceeded	0
xSec users	0
xSec tunnel	0

### License Table

Key	Installed	Expires	Flags	Service Type	Actions
rAj0GBvJ-NAY0Fhr8-4xd1V5ky-N9OXVb2w-40JQ6BPN-U84	2009-03-13 12:10:07	Never	E	Access Points: 32	Delete
Qs6QncVT-QTaRc9iS-At7hvQNm-ThjHKmjD-lWmTSEly-VsY	2011-08-03 06:54:54	Never	E	Next Generation Policy Enforcement Firewall Module: 32	Delete

Flags: A - auto-generated; E - enabled; R - reboot required to activate

Add New License Key

Add

Save Report Export Database Import Database

## Logical and Physical Interfaces

This section defines the Layer-2/3 framework that connects the Spectralink phones with the assigned Spectralink Gateway and SVP server through WLAN Mobility Controller (MC) and the Access Points. *The requirement is that the phones and Spectralink infrastructure be connected over Layer-2 and have the L2 subnet span across L3 switching/routing fabric.*

The steps involved are

- 1 Define a VLAN for voice on the WLAN.
- 2 Define the IP parameters for the VLAN.
- 3 Define the DHCP server for the phones to get their IP addresses.
- 4 Define the physical port assignment on the MC. Most deployments have the MC uplinked to a Layer-3 switch which performs routing functions.

These parameters can be easily defined using the Controller Wizard on the WebUI.

### Using CLI

#### IP Interfaces, VLAN configuration

```
(Aruba651) #configure terminal

(Aruba651) (config) #vlan <vlan ID>
(Aruba651) (config) #interface <vlan ID>
(Aruba651) (config-subif)#ip address <VLAN interface IP> <subnet mask>
(Aruba651) (config-subif)#ip helper-address <DHCP server / helper for the VLAN>
(Aruba651) (config-subif)#write m
(Aruba651) (config-subif)#end
```

#### Physical Port Assignment

The uplink is configured as follows

```
(Aruba651) (config) #interface gigabitethernet <slot/port>
(Aruba651) (config-if)#trusted
(Aruba651) (config-if)#no shutdown
(Aruba651) (config-if)#switchport mode trunk
(Aruba651) (config-if)#switchport trunk allowed vlan <VLAN IDs>
(Aruba651) (config-if)#write memory
```

#### On the WebUI

- 1 Click the **Configuration** tab.



- 2 On the left pane, click **Controller** under **WIZARDS**.
- 3 The **Basic Info** and **Licenses** fields should be auto-filled from the Initialization steps. Click **Next** on both to arrive at the **VLANs** and **IP Interfaces** page.
- 4 Highlight the default VLAN line and click on it. (Other VLAN's may be entered here: see Aruba documentation for details.)
- 5 Enter details for the VLAN on which the phones are desired – VLAN ID, VLAN-Name.
  - a Click the drop-down to enter an IP address for the VLAN interface on the controller and the subnet mask. (Please bear in mind that L2 connectivity is required for the phones to reach the voice server and gateway).
  - b Click to choose the ports assigned to the VLAN (default is all available ports).
  - c Specify details on how the phones are expected to get their IP addresses. This drop-down offers the option of static IP assignment (**None**), DHCP using the in-built DHCP server (**Act as server**) and DHCP using an external DHCP server (**Relay to external**).

Named VLANs		All VLAN IDs on This Controller				
All		ID	IP Address/Netmask	Enable NAT	Port Members	DHCP Settings
		1	172.29.109.108/255.255.255.128	<input type="checkbox"/>	1/0,1/1,1/2,1/3	<input checked="" type="radio"/> None <input type="radio"/> Relay to external <input type="radio"/> Act as server

- 6 Click **Save Configuration**

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

**Configure Controller**

Workflow Help

- Basic Info  
Name: Aruba3600
- Licenses  
License Installed:2
- VLANs and IP Interfaces**
- Connectivity
- Uplink
- Ports
- Finish

### Configure VLANs and IP Interfaces for Aruba3600

Configure VLANs for this controller. [More...](#)

Named VLANs		All VLAN IDs on This Controller				
	All	ID	IP Address/Netmask	Enable NAT	Port Members	DHCP Settings
		1	172.29.109.108/255.255.255.128	--	all	None

New Delete Add Delete

Back Next Cancel

- 7 Click **Next** to proceed to Connectivity assignment.
  - a Enter the IP address for the Default Gateway or pick Dynamic if the default gateway will be provided by DHCP, DNS, or router infrastructure.
  - b Click **Next** to proceed to physical port assignment.
- 8 On **Ports**, enter the following
  - a By default, all ports are on VLAN 1. To change port configuration, click the corresponding row.
  - b If the controller has a single uplink to the wired network, check the Trunk Mode box for the port and include the VLANs to be trunked on that port.
  - c If the controller has only one uplink, STP should be disabled.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

**Configure Controller**

Workflow Help

- 1 Basic Info  
Name: Aruba3600
- 2 Licenses  
License Installed: 2
- 3 VLANs and IP Interfaces  
VLAN Names: 0
- 4 Connectivity  
Default Gateway: 172.29.109.1
- 5 Uplink  
Uplink Ports:  
Uplink firewall: Disabled
- 6 **Ports**
- 7 Finish

### Configure Ports for Aruba3600

Settings for all ports are shown in the table below. Select any row to edit it. [More...](#)

Fast Ethernet						
Port	Enabled	Trusted	Speed/Duplex	Native VLAN	Trunk Mode	VLANs for Trunk Mode

Gigabit Ethernet (edited)							Reset
Port	Enabled	Trusted	Speed/Duplex	Native VLAN	Trunk Mode	VLANs for Trunk Mode	
1/0	✓	✓	auto/auto	1	✓	--	
1/1	✓	✓	auto/auto	1	✓	--	
1/2	✓	✓	auto/auto	1	✓	--	
1/3	✓	✓	auto/auto	1	✓	--	

STP for all ports: Enabled NOTE: STP should be disabled if this Controller has only single uplink to the network

Back Next Cancel

9 Click **Next** twice, then click finish to save the changes to the configuration.

## *Creating Firewall Roles and Policies*

The Aruba MC has an application-aware stateful firewall that can assign prioritization to Spectralink voice traffic once it knows that a certain wireless client is a Spectralink handset. This is accomplished by the following steps:

- 1** Create a user role that the phones should be assigned to.
- 2** Create the syslog policy.
- 3** Assign firewall policies to the role
- 4** Create a user-derivation rule that dictates how a client should be identified as a Spectralink voice phone. In this case it is easiest to classify based on the leading octets of the MAC OUI (00:90:7a).
- 5** Finally, create an AAA-profile that ties the user-derivation rule with the appropriate firewall rules.

## Creating a Syslog Policy

### On CLI

```
(Aruba651) (config) #ip access-list session syslog
```

```
(Aruba651) (config-sess-syslog) #any any svc-syslog permit
```

### On WebUI

- 1 Click the Configuration tab.
- 2 Click Access Control.
- 3 Click Policies.
- 4 Click Add.

The screenshot shows the Aruba Mobility Controller WebUI interface. The top navigation bar includes 'Dashboard', 'Monitoring', 'Configuration' (selected), 'Diagnostics', 'Maintenance', and 'Plan'. A 'Save Configuration' button is also present. The left sidebar lists various configuration categories like WIZARDS, NETWORK, SECURITY, and MANAGEMENT. The main content area is titled 'Security > Access Control > Firewall Policies'. Below this title are tabs for 'User Roles', 'System Roles', 'Policies' (selected), 'Time Ranges', and 'Guest Access'. A table lists existing policies with columns for Name, Type, Rule Count, Policy Usage, and Action. The table includes policies like 'validuser', 'sys-control', 'sys-ap-ad', 'stateful-dot1x', 'ap-uplink-ad', 'allow-diskaervices', 'allow-printservices', 'control', 'logon-control', and 'ap-acl'. Each policy has 'Edit' and 'Delete' buttons. At the bottom of the table, there is a pagination control showing '1 2 2 Next | 1-10 of 28' and a dropdown menu set to '10'. An 'Add' button is located at the bottom left of the table area.

Name	Type	Rule Count	Policy Usage	Action
validuser	session	3		Edit Delete
sys-control	session	9	sys-ap-role	Edit Delete
sys-ap-ad	session	10	sys-ap-role	Edit Delete
stateful-dot1x	session	2		Edit Delete
ap-uplink-ad	session	4		Edit Delete
allow-diskaervices	session	3		Edit Delete
allow-printservices	session	3		Edit Delete
control	session	10	ap-role	Edit Delete
logon-control	session	5	logon guest-logon	Edit Delete
ap-acl	session	6	ap-role	Edit Delete

- 5 Set the Policy name to **syslog**, the policy type to **Session**, the service to **service**, the service name to **svc-syslog (udp-514)**, and the action to **permit**.

ARUBA NETWORKS MOBIILITY CONTROLLER | Aruba3600VIEW

Dashboard Monitoring **Configuration** Diagnostics Maintenance Plan [Save Configuration](#) [Logout admin](#)

WIZARDS  
AP Wizard  
Controller Wizard  
WLAN/LAN Wizard  
License Wizard

NETWORK  
Controller  
VLANs  
Ports  
Cellular Profile  
IP

SECURITY  
Authentication  
Access Control

WIRELESS  
AP Configuration  
AP Installation

MANAGEMENT  
General  
Administration  
Certificates  
SNMP  
Logging  
Clock  
Guest Provisioning  
Captive Portal  
SMTP  
Bandwidth Calculator

ADVANCED SERVICES  
Redundancy  
IP Mobility  
Stateful Firewall  
External Services  
VPN Services  
Wired Access  
Wireless  
All Profiles

**Security > Firewall Policies > Add New Policy**

User Roles System Roles **Policies** Time Ranges Guest Access

Policy Name: syslog  
Policy Type: Session

Rules

IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	Pause ARM Scanning	BlackList	Classify Media	TOS	802.1p Priority	Action
IP Version	Source	Destination	Service	Action	Log	Mirror	Queue	Time Range	Pause ARM Scanning	Black List	Classify Media	TOS	802.1p Priority	
IPv4	any	any	Service	permit	<input type="checkbox"/>	<input type="checkbox"/>	High		<input type="checkbox"/>					
<div> <div> Add Cancel </div> <div> Apply </div> </div>														

Commands

View Commands

Service

- svc-netbios-dgm (udp 138)
- svc-nat (udp 4500)
- svc-netbios-dgm (udp 138)
- svc-netbios-na (udp 137)
- svc-netbios-ssn (tcp 139)
- svc-noe (udp 32512)
- svc-noe-ova (udp 5000)
- svc-nterm (tcp 1026-1028)
- svc-ntp (udp 123)
- svc-pap (udp 8211)
- svc-pop3 (tcp 110)
- svc-pptp (tcp 1723)
- svc-rtsp (tcp 554)
- svc-scp (tcp 2000)
- svc-sec-pap (udp 8209)
- svc-sftp (tcp 5061)
- svc-sip-tcp (tcp 5060)
- svc-sip-udp (udp 5060)
- svc-smb-tcp (tcp 445)
- svc-smb-udp (udp 445)
- svc-smtp (tcp 25)
- svc-snmp (udp 161)
- svc-snmp-trap (udp 162)
- svc-ssh (tcp 22)
- svc-svp (119 0)
- svc-syslog (tcp 514)
- svc-telnet (tcp 23)
- svc-tftp (udp 69)
- svc-v6-dhcp (udp 546-547)
- svc-v6-icmp (icmpv6 0)
- svc-vocera (udp 5002)

## 6 Click **Add**, then **Apply**.


## Creating User-Role and Assigning Firewall Rules to the Role

### On CLI

```
(Aruba651) (config) #user-role spectralink
(Aruba651) (config-role) #access-list session svp-acl position 1
(Aruba651) (config-role) #access-list session sip-acl position 2
(Aruba651) (config-role) #access-list session tftp-acl position 3
(Aruba651) (config-role) #access-list session icmp-acl position 4
(Aruba651) (config-role) #access-list session dhcp-acl position 5
(Aruba651) (config-role) #access-list session syslog position 6
(Aruba651) (config-role) #access-list session dns-acl position 6
```

### On WebUI

- 1 Click the **Configuration** tab.
- 2 Click **Access Control**.
- 3 Click **Add**
- 4 Assign a Role-name for the phones (Ex. spectralink).
- 5 Under **Firewall Policies**, click **Add**.
- 6 Click **Choose** from configured policies radio-button.
- 7 From the drop-down list, choose **svp-acl sip-acl, tftp-acl, icmp-acl, dhcp-acl, dns-acl**, and **syslog** policies to the list, clicking **Done** after each selection and repeating from step 5.
- 8 Click **Apply** at the bottom of the page.
- 9 Click **Save Configuration**.



Configuration

Monitoring | Configuration | Diagnostics | Maintenance | Plan | Events | Reports | Licenses will expire in 28 days | Save Configuration | Logout admin

**Wizards**

- Controller Wizard
- WLAN Wizard
- License Wizard

**Network**

- Controller
- VLANs
- Ports
- IP

**Security**

- Authentication
- Access Control**

**Wireless**

- AP Configuration
- AP Installation

**Management**

- General
- Administration
- Certificates
- SNMP
- Logging
- Clock

**Advanced Services**

- Redundancy
- IP Mobility
- Stateful Firewall
- Wired Access
- Wireless
- All Profiles

### Security > User Roles > Add Role

User Roles | System Roles | Policies | Time Ranges | Guest Access

< Back

Role Name: Polycorn

#### Firewall Policies

Name	Rule Count	AP Group	Action
<a href="#">Add</a>			
<input checked="" type="radio"/> Choose from Configured Policies: <input type="text" value="svp-acl (session)"/> AP Group: <input type="text"/>			
<input type="radio"/> Create New Policy From Existing Policy: <input type="text" value="validuser (session)"/> <a href="#">Create</a>			
<input type="radio"/> Create New Policy <a href="#">Create</a>			
<a href="#">Done</a> <a href="#">Cancel</a>			

#### Re-authentication Interval

Disabled [Change](#) (0 disables re-authentication. A positive value enables authentication 0 - 4096 )

#### Role VLAN ID

Not Assigned  [Change](#)

#### Bandwidth Contract

Upstream: Not Enforced  [Change](#) ☐ Per User

Downstream: Not Enforced  [Change](#) ☐ Per User




## Creating a User-Role Derivation Rule

### On CLI

```
(Aruba651) (config) # aaa derivation-rules user spectralink-derivation
(Aruba651) (user-rule) #set role condition macaddr starts-with 00:90:7a
set-value spectralink
(Aruba651) (user-rule) # write memory
```

### On WebUI

- 1 Click the **Configuration** tab.
- 2 Click **Authentication**.
- 3 Click **User Rules** and click **Add**.
- 4 Type a name for the user rules, such as spectralink-derivation.
- 5 Click **Add**.
- 6 Click the newly entered name in the tree in the left column.
- 7 Click **Add**.
  - a Fill the following parameters
  - b **Set Type – Role**
  - c **Rule Type – MAC Address**
  - d **Condition – starts with**
  - e **Value – 00:90:7a**
  - f **Roles** – <select role created for phones> (spectralink in this example).
- 8 Click **Add** and then **Apply**.
- 9 Click **Save Configuration**.



Configuration

Monitoring | Configuration | Diagnostics | Maintenance | Plan | Events | Reports | Licenses will expire in 28 days | Save Configuration | Logout admin

**Wizards**

- Controller Wizard
- WLAN Wizard
- License Wizard

**Network**

- Controller
- VLANs
- Ports
- IP

**Security**

- Authentication
- Access Control**

**Wireless**

- AP Configuration
- AP Installation

**Management**

- General
- Administration
- Certificates
- SNMP
- Logging
- Clock

**Advanced Services**

- Redundancy
- IP Mobility
- Stateful Firewall
- Wired Access
- Wireless
- All Profiles

### Security > User Roles > Add Role

User Roles | System Roles | Policies | Time Ranges | Guest Access

< Back

Role Name: Polycorn

#### Firewall Policies

Name	Rule Count	AP Group	Action
<a href="#">Add</a>			
<input checked="" type="radio"/> Choose from Configured Policies: <input type="text" value="svp-acl (session)"/> AP Group: <input type="text"/>			
<input type="radio"/> Create New Policy From Existing Policy: <input type="text" value="validuser (session)"/> <a href="#">Create</a>			
<input type="radio"/> Create New Policy <a href="#">Create</a>			
<a href="#">Done</a> <a href="#">Cancel</a>			

#### Re-authentication Interval

Disabled  [Change](#) (0 disables re-authentication. A positive value enables authentication 0 - 4096 )

#### Role VLAN ID

Not Assigned  [Change](#)

#### Bandwidth Contract

Upstream: Not Enforced  [Change](#) ☐ Per User

Downstream: Not Enforced  [Change](#) ☐ Per User

## Configuration Steps for None, WEP, WPA-PSK or WPA2-PSK Security

### Creating an Authentication Profile for controller-based authentication

#### On CLI

```
(Aruba651) (config) # aaa authentication dot1x default
(Aruba651) (802.1X Authentication Profile "default") #termination enable
(Aruba651) (802.1X Authentication Profile "default") #termination eap-type
eap-peap
(Aruba651) (802.1X Authentication Profile "default") #termination inner-
eap-type eap-mschapv2
(Aruba651) (802.1X Authentication Profile "default") #exit
(Aruba651) (config) aaa authentication dot1x "spectralink-psk"
(Aruba651) (802.1X Authentication Profile "spectralink-psk") #machine-
authentication machine-default-role spectralink
(Aruba651) (802.1X Authentication Profile "spectralink-aaa") #machine-
authentication user-default-role spectralink
(Aruba651) (802.1X Authentication Profile "spectralink-aaa") #timer
idrequest_period 65535
(Aruba651) (802.1X Authentication Profile "spectralink-aaa")
#exit

(Aruba651) #configure terminal aaa profile spectralink-aaa
(Aruba651) (AAA Profile "spectralink-aaa") #initial-role authenticated
(Aruba651) (AAA Profile "spectralink-aaa") #authentication-dot1x
spectralink-psk
(Aruba651) (AAA Profile "spectralink-aaa") #user-derivation-rules
spectralink-derivation
```

#### On WebUI

- 1 Navigate to **Configuration** and **Authentication**.
- 2 Click the **L2-Authentication** tab.
- 3 Click **802.1X Authentication Profile** in the middle-pane to expand the tree and click **default**.
  - a On the right pane, check **Termination**.
  - b For **Termination EAP-Type**, click **eap-peap**.
  - c For **Termination Inner EAP-Type**, check **eap-mschapv2**.

**d Click Apply.**

Dashboard | Monitoring | **Configuration** | Diagnostics | Maintenance | Save Configuration

WIZARDS  
AP  
Controller  
Campus WLAN  
Remote AP  
AirWave  
NETWORK  
Controller  
VLANs  
Ports  
Cellular Profile  
IP  
SECURITY  
> **Authentication**  
Access Control  
WIRELESS  
AP Configuration

**Security > Authentication > Profiles**

Servers | **AAA Profiles** | L2 Authentication | L3 Authentication | User Rules | Advanced

AAA  
☐ default  
☐ default-dot1x  
     MAC Authentication  
     MAC Authentication Server Group default  
     **802.1X Authentication** default  
     802.1X Authentication Server Group  
     RADIUS Accounting Server Group  
☐ XML API server  
☐ RFC 3576 server  
☐ default-dot1x-psk  
☐ default-mac-auth

**802.1X Authentication Profile > default** Show Reference Save As Reset

Basic Advanced

Max authentication failures	0	
Enforce Machine Authentication	<input type="checkbox"/>	
Machine Authentication: Default Machine Role	guest	
Machine Authentication: Default User Role	guest	
Reauthentication	<input type="checkbox"/>	
Termination	<input checked="" type="checkbox"/>	
Termination EAP-Type	<input type="checkbox"/> eap-tls	<input checked="" type="checkbox"/> eap-peap
Termination Inner EAP-Type	<input checked="" type="checkbox"/> eap-mschapv2	<input type="checkbox"/> eap-gtc

- 4** Click the **AAA Profiles** page and on the right-pane, click **Add**.
- 5** Assign a name to the AAA profile (Ex. spectralink-aaa) and click **Add**.
- 6** Click the newly created profile name.
- 7** Edit the AAA profile
  - a** Drop-down the list against **User derivation rules** and select the rule created for the Spectralink phones.
  - b** Click **Apply**.

Dashboard | Monitoring | **Configuration** | Diagnostics | Maintenance | Save Configuration

WIZARDS

- AP
- Controller
- Campus WLAN
- Remote AP
- AirWave

NETWORK

- Controller
- VLANs
- Ports
- Cellular Profile
- IP

SECURITY

- > **Authentication**
  - Access Control

WIRELESS

- AP Configuration
- AP Installation

MANAGEMENT

- General
- Administration
- Certificates
- SNMP
- Logging
- Clock
- Guest Provisioning
- Captive Portal
- SMTP
- Bandwidth Calculator
- Threshold

ADVANCED SERVICES

- Redundancy
- AirGroup
- IP Mobility
- Stateful Firewall
- External Services
- VPN Services
- Wired Access
- All Profiles
- [E-mail Support](#)

**Security > Authentication > Profiles**

Servers | **AAA Profiles** | L2 Authentication | L3 Authentication | User Rules | Advanced

AAA

- default
- default-dot1x
  - MAC Authentication
  - MAC Authentication Server Group default
  - 802.1X Authentication default
  - 802.1X Authentication Server Group
  - RADIUS Accounting Server Group
- XML API server
- RFC 3576 server
- default-dot1x-psk
- default-mac-auth
- default-open
- default-xml-api
- NoAuthAAAProfile
- spectralink-aaa**
  - MAC Authentication
  - MAC Authentication Server Group default
  - 802.1X Authentication spectralink-psk
  - 802.1X Authentication Server Group
  - RADIUS Accounting Server Group
  - XML API server
  - RFC 3576 server
  - spectralink-dot1x

**AAA Profile > spectralink-aaa** Show Reference Save As Reset

Initial role	authenticated
MAC Authentication Default Role	guest
802.1X Authentication Default Role	guest
L2 Authentication Fail Through	<input type="checkbox"/>
User idle timeout	<input type="checkbox"/> Enable seconds
RADIUS Interim Accounting	<input type="checkbox"/>
User derivation rules	spectralink-derivation
Wired to Wireless Roaming	<input checked="" type="checkbox"/>
SIP authentication role	--NONE--
Device Type Classification	<input checked="" type="checkbox"/>
Enforce DHCP	<input type="checkbox"/>

Commands Apply View Commands

- 8 Click on **802.1X Authentication** underneath the **spectralink-aaa** profile entry.
  - a Click the **Advanced** tab.
  - b By **802.1X Authentication Profile**, click on **--NEW--**.
  - c Enter a name in the box by **--NEW--**, **spectralink-psk**.
  - d From the drop down list by **Machine Authentication: Default Machine Role**, select the role created earlier, **spectralink**.
  - e From the drop down list by **Machine Authentication: Default User Role**, select the role created earlier, **spectralink**.
  - f Set the Interval between Identity Requests to **65535**.
  - g Click **Apply**.
  - h Click **Save Configuration**.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave

NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP

SECURITY  
**> Authentication**

WIRELESS  
 AP Configuration  
 AP Installation

MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP

Bandwidth Calculator  
 Threshold

ADVANCED SERVICES  
 Redundancy  
 AirGroup  
 IP Mobility  
 Stateful Firewall  
 External Services  
 VPN Services  
 Wired Access  
 All Profiles  
[E-mail Support](#)

**Security > Authentication > Profiles**

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

AAA

- default
- default-dot1x
  - MAC Authentication
    - MAC Authentication Server Group default
    - 802.1X Authentication default
    - 802.1X Authentication Server Group
    - RADIUS Accounting Server Group
  - XML API server
  - RFC 3576 server
- default-dot1x-psk
- default-mac-auth
- default-open
- default-xml-api
- NoAuthAAAProfile
- spectralink-aaa
  - MAC Authentication
    - MAC Authentication Server Group default
    - 802.1X Authentication spectralink-psk**
    - 802.1X Authentication Server Group
    - RADIUS Accounting Server Group
  - XML API server
  - RFC 3576 server
  - spectralink-dot1x

**802.1X Authentication Profile > spectralink-psk** Show Reference Save As Reset

Basic Advanced

Max authentication failures	0
Enforce Machine Authentication	<input type="checkbox"/>
Machine Authentication: Default Machine Role	spectralink
Machine Authentication Cache Timeout	24 hr(s)
Blacklist on Machine Authentication Failure	<input type="checkbox"/>
Machine Authentication: Default User Role	spectralink
Interval between Identity Requests	65535 sec
Quiet Period after Failed Authentication	30 sec
Reauthentication Interval	86400 sec
Use Server provided Reauthentication Interval	<input type="checkbox"/>
Use the termination-action attribute from the Server	<input type="checkbox"/>
Multicast Key Rotation Time Interval	1800 sec
Unicast Key Rotation Time Interval	900 sec
Authentication Server Retry Interval	5 sec
Authentication Server Retry Count	3
Framed MTU	1100 bytes
Number of times ID-Requests are retried	5
Maximum Number of Reauthentication Attempts	3
Maximum number of times Held State can be bypassed	0
Dynamic WEP Key Message Retry Count	1
Dynamic WEP Key Size	128 bits
Interval between WPA/WPA2 Key Messages	1000 msec
Delay between EAP-Success and WPA2 Unicast Key Exchange	0 msec
Delay between WPA/WPA2 Unicast Key and Group Key Exchange	0 msec
Time interval after which the PMKSA will be deleted	8 hr(s)
Delete Keycache upon user deletion	<input type="checkbox"/>
WPA/WPA2 Key Message Retry Count	3
Multicast Key Rotation	<input type="checkbox"/>
Unicast Key Rotation	<input type="checkbox"/>

Apply

**Commands** View Commands

## Configuration Steps for WPA2-Enterprise Security

### Defining an 802.1X authentication server

#### On CLI

```
(Aruba651) (config) #aaa authentication-server RADIUS <server-group name>
(Aruba651) (RADIUS Server "spectralink-dot1x") #host <server IP>
(Aruba651) (RADIUS Server "spectralink-dot1x") #key <RADIUS secret>
(Aruba651) (RADIUS Server "spectralink-dot1x") #write memory
```

#### On WebUI

- 1 Navigate to **Configuration** and **Authentication**.
- 2 Click **RADIUS Server**, name server profile (Ex. Spectralink-dot1x) and click **Add**.
- 3 Click the newly created instance to configure.
- 4 Input the IP address of the external RADIUS server and the secret.



#### **Settings: Define Aruba Controller on Radius with the same secret**

The Aruba mobility controller should be defined as a dot1x client on the RADIUS server and configured with the same secret as in step 4 above.

- 5 Click **Apply** and **Save Configuration**.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave  
 NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP  
 SECURITY  
 > **Authentication**  
 Access Control  
 WIRELESS  
 AP Configuration  
 AP Installation  
 MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold  
 ADVANCED SERVICES  
 Redundancy  
 AirGroup  
 IP Mobility

**Security > Authentication > Servers**

Servers AAA Profiles L2 Authentication L3 Authentication User Rules Advanced

Server Group  
 RADIUS Server  
 CiscoACS

LDAP Server  
 Internal DB  
 Tacacs Accounting Server  
 TACACS Server  
 XML API Server  
 RFC 3576 Server  
 Windows Server

**RADIUS Server > CiscoACS** Show Reference Save As Reset

Host 172.29.65.19

Key  
 Retype:

Auth Port 1812

Acct Port 1813

Retransmits 3

Timeout 5 sec

NAS ID

NAS IP

Enable IPv6 ☐

NAS IPv6

Source Interface vlanid ipv6addr

Use MD5 ☐

Use IP address for calling station ID ☐

Mode ☒

Lowercase MAC addresses ☐

MAC address delimiter none

Service-type of FRAMED-USER ☐

Commands Apply View Commands



## Settings: Define OKC on the handset

**Fast roaming** must be set to **Opportunistic Key Caching (OKC)** on the handset when WPA2-Enterprise is in use. It is enabled by default on the controller.



## Create a Server Group and Add the RADIUS Server

### Using CLI

```
(Aruba651) #configure terminal
(Aruba651) (config) #aaa server-group < Server Name > (Ex.Spectralink)
(Aruba651) (Server Group "Spectralink") # auth-server "Spectralink-dot1x"
position 1
(Aruba651) (Config) #aaa profile "Spectralink-dot1x"
(Aruba651) (AAA Profile ""Spectralink-dot1x") #dot1x-server-group
"Spectralink"
```

### Using WebUI

- 1 Navigate to **Configuration** and **Authentication**.
- 2 Click the **Servers** tab. Click the **Server Group**.
- 3 In the right pan click **Add** and create a new server group (Ex. Spectralink).
- 4 Click the newly created server group.
- 5 Click **New** under **Servers** tab.
- 6 Assign the required RADIUS server under **Server Name**, click **Add Server** and **Apply** button.

## Creating an 802.1X Authentication Profile

### Using CLI

```
(Aruba651) (config) #aaa authentication dot1x <profile-name>
```

#### If termination is required

```
(Aruba651) (802.1X Authentication Profile "spectralink-dot1x") #termination  
enable
```

```
(Aruba651) (802.1X Authentication Profile "spectralink-dot1x") #termination  
eap-type eap-peap
```

```
(Aruba651) (802.1X Authentication Profile "spectralink-dot1x") #termination  
inner-eap-type eap-mschapv2
```

### Using WebUI

- 1 Navigate to **Configuration** and **Authentication**.
- 2 Click the **L2 Authentication** tab.
- 3 Click **Add** and create a new profile (Ex. spectralink-dot1x).
- 4 Click **802.1X Authentication** tab.
- 5 Click the newly created instance and enable termination. Specify the **EAP type** to be **eap-peap** and the **Inner-EAP type** to be **eap-mschapv2**.
- 6 Click **Apply** and **Save Configuration**.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
AP  
Controller  
Campus WLAN  
Remote AP  
AirWave  
NETWORK  
Controller  
VLANs  
Ports  
Cellular Profile  
IP  
SECURITY  
➤ **Authentication**  
Access Control  
WIRELESS  
AP Configuration  
AP Installation  
MANAGEMENT  
General  
Administration  
Certificates  
SNMP  
Logging  
Clock  
Guest Provisioning  
Captive Portal  
SMTP  
Bandwidth Calculator  
Threshold  
ADVANCED SERVICES  
Redundancy  
AirGroup

**Security > Authentication > L2 Authentication**

Servers AAA Profiles **L2 Authentication** L3 Authentication User Rules Advanced

MAC Authentication  
802.1X Authentication  
default  
default-psk  
**spectralink-802.1x**  
spectralink-psk  
Stateful 802.1X Authentication

**802.1X Authentication Profile > spectralink-802.1x** Show Reference Save As Reset

Basic Advanced

Max authentication failures	0
Enforce Machine Authentication	<input type="checkbox"/>
Machine Authentication: Default Machine Role	spectralink
Machine Authentication: Default User Role	spectralink
Reauthentication	<input type="checkbox"/>
Termination	<input checked="" type="checkbox"/>
Termination EAP-Type	<input type="checkbox"/> eap-tls <input checked="" type="checkbox"/> eap-peap
Termination Inner EAP-Type	<input checked="" type="checkbox"/> eap-mschapv2 <input type="checkbox"/> eap-gtc

Apply

**Commands** View Commands

## Creating an Authentication Profile

### Using CLI

```
(aruba86) #configure terminal aaa profile <profile-name>
(aruba86) (AAA Profile "spectralink-dot1x") #authentication-dot1x <post-
authentication role name>
(aruba86) (AAA Profile "spectralink-dot1x") #dot1x-server-group <dot1x
authentication server name>
```

### Using WebUI

- 1 Navigate to **Configuration** and **Authentication**.
- 2 Click the **AAA Profiles** tab.
- 3 Click **Add** and create a new profile (Ex. spectralink-dot1x).
- 4 Expand the newly created profile.
- 5 Change the **User derivation rules** (Ex. spectralink-derivation) to the user-role created for the phones.
- 6 Click **802.1X Authentication Profile** and specify the newly created profile.
- 7 Click **Apply** and **Save Configuration**.

ARUBA networks MOILITY CONTROLLER | Aruba3600 [Log out admin](#)

Dashboard Monitoring **Configuration** Diagnostics Maintenance [Save Configuration](#)

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave  
 NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP  
 SECURITY  
**> Authentication**  
 Access Control  
 WIRELESS  
 AP Configuration  
 AP Installation  
 MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold  
 ADVANCED SERVICES  
 Redundancy

**Security > Authentication > Profiles**

Servers AAA Profiles **L2 Authentication** L3 Authentication User Rules Advanced

MAC Authentication

MAC Authentication Server Group default

802.1X Authentication default -psk

802.1X Authentication Server Group

RADIUS Accounting Server Group

☐ XML API server

☐ RFC 3576 server

☐ default-mac-auth

☐ default-open

☐ default-xml-api

☐ NoAuthAAAProfile

☐ spectralink-aaa

☒ **spectralink-dot1x**

MAC Authentication

MAC Authentication Server Group default

802.1X Authentication spectralink -802.1x

802.1X Authentication Server Group RADIUS

RADIUS Accounting

**AAA Profile > spectralink-dot1x** [Show Reference](#) [Save As](#) [Reset](#)

Initial role logon

MAC Authentication Default Role guest

802.1X Authentication Default Role guest

L2 Authentication Fail Through ☐

User idle timeout ☐ Enable seconds

RADIUS Interim Accounting ☐

User derivation rules spectralink-derivation

Wired to Wireless Roaming ☒

SIP authentication role --NONE--

Device Type Classification ☒

Enforce DHCP ☐

[Apply](#) [View Commands](#)

**Commands**

## Wireless LAN Configuration

This section defines the wireless network parameters that are most aptly suited to the Spectralink phones.

It is required to have separate SSID for the Spectralink phones and other data clients. Also, certain parameters need to be modified to allow seamless interoperability of Spectralink phones in and off-call with Aruba's Adaptive Radio Management (ARM) mechanism. Aruba OS accomplishes this by creating independent profiles for the SSID definition, radio definition and ARM definitions before tying them together to an AP-group on which they would operate. This way, all APs configured to be part of the AP-group will have the same operational parameters. The steps in this procedure are below

- 1 Create an SSID profile – each SSID profile is characterized by the ESSID and the authentication-encryption scheme.
- 2 Create a HT-SSID profile (with 802.11n features disabled) and assign the HT-SSID to the SSID profile.
- 3 Create a Virtual-AP profile that ties the SSID profile and authentication profile (created in the previous section) with a VLAN on the wired-side.
- 4 Create Radio-profiles for the 2.4 GHz and 5 GHz radio. This would include ARM and HT-Radio profile settings. In this example, we modify the default radio profiles which are assigned to the Virtual-AP automatically.
- 5 Associate the Virtual-AP with an AP-group.

The WLAN configuration for 802.1X authentication is identical to that for PSK-based authentication except for the following 2 points

- In Creating a SSID-profile, op-mode on the SSID should be set to **wpa2-aes**.
- The AAA profile for the Virtual-AP should be set to the newly created **dot1x** profile (spectralink-dot1x).

### On CLI

#### Creating a SSID-profile

```
(Aruba651) #configure terminal wlan ssid-profile view
```

```
For None (open network - no security) #opmode opensystem
```

```
For WEP
```

```
(Aruba651) (SSID Profile "view") #opmode static-wep
```

```
(Aruba651) (SSID Profile "view") #weptxkey <index 1-4>
```

```
(Aruba651) (SSID Profile "view") #wepkey<index> <"string of hex characters">
```

For WPA-PSK

```
(Aruba651) (SSID Profile "view") #opmode wpa-psk-tkip
(Aruba651) (SSID Profile "view") #wpa-passphrase <"passphrase">
```

For WPA2-PSK

```
(Aruba651) (SSID Profile "view") #opmode wpa2-aes-psk
(Aruba651) (SSID Profile "view") #wpa-passphrase <"passphrase">
```

For all

```
(Aruba651) (SSID Profile "view") #dtim-period 2
(Aruba651) (SSID Profile "view") #no wmm
(Aruba651) (SSID Profile "view") #no wmm-uapsd
(Aruba651) (SSID Profile "view") #strict-svp
(Aruba651) (SSID Profile "view") #essid view
(Aruba651) (SSID Profile "view") #a-tx-rates 6 9 12 18 24 36 48 54
(Aruba651) (SSID Profile "view") #g-basic-rates 5
(Aruba651) (SSID Profile "view") #g-tx-rates 5 6 11 12 18 24 36 48 54
(Aruba651) (SSID Profile "view") #max-tx-fail 0
```

## Creating a Virtual-AP

```
(Aruba651) #configure terminal wlan virtual-ap spectralink-vap
(Aruba651) (Virtual AP Profile "spectralink-vap") #no broadcast-filter arp
(Aruba651) (Virtual AP Profile "spectralink-vap") #vlan 1
```

## HT-SSID profile (disable 802.11n network)

```
(Aruba651) #configure terminal wlan ht-ssid-profile ht-disabled
(Aruba651) (High-throughput SSID profile "ht-disabled") #no high-
throughput-enable
(Aruba651) (High-throughput SSID profile "ht-disabled") #no 40MHz-enable
(Aruba651) (High-throughput SSID profile "ht-disabled") #no mpdu-agg
```

## Assigning HT-SSID and EDCA profiles to the SSID-Profile

```
(Aruba651) #configure terminal wlan ssid-profile view
(Aruba651) (SSID Profile "view") #ht-ssid-profile <ht-disabled or ht-
enabled>
(Aruba651) (SSID Profile "view") #edca-parameters-profile station <AC_OFF
or AC_ON>
(Aruba651) (SSID Profile "view") #edca-parameters-profile ap <AC_OFF or
AC_ON>
```

## Adding the aaa-profile and the ssid-profile to the virtual-ap profile

```
(Aruba651) (config) #wlan virtual-ap spectralink-vap
(Aruba651) (Virtual AP profile "spectralink-vap") #aaa-profile spectralink-aaa
(Aruba651) (Virtual AP profile "spectralink-vap") #ssid-profile spectralink-dot1x
```

## Creating Radio profiles

In most cases, one can use the default Radio-profile, HT-Radio profile and ARM profile and modify them as required. If there are multiple AP-groups on the network that require different radio profiles, please refer to the ArubaOS User Guide to create and assign radio-profiles to AP-Groups.

### 5 GHz Radio settings

```
(Aruba651) (config) #rf dot11a-radio-profile default
```

#### Enable or disable 5 GHz radio

```
(Aruba651) (802.11a radio profile "default")#<no> radio-enable
```

#### Choose a channel

```
(Aruba651) (802.11a radio profile "default")#channel <desired channel>
```

#### Enable 80 MHz or not

```
(Aruba651) (802.11a radio profile "default")#<no> very-high-throughput enable
```

Note: the AP must be power cycled for the 80 MHz setting to take effect.

#### Enable 40 MHz or not

```
(Aruba651) (802.11a radio profile "default")#<no> high-throughput enable
```



### Admin Tip: Transmit Power

For setting up the **Transmit Power**, please consult your facility's RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. Spectralink Wireless Telephones require the following minimum dBm reading to support the corresponding **Mandatory** data rate setting in the access point.

802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum "Mandatory" Data Rate
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s





### Web Info: RF Deployment reference

For additional details on RF deployment please see the *Deploying Enterprise-Grade Wi-Fi Telephony White Paper*.

```
(Aruba651) (802.11a radio profile "default") #tx-power <transmit EIRP in .5 dBm increments)
```

```
(Aruba651) (802.11a radio profile "default") #no spectrum-load-balancing
```

```
(Aruba651) (802.11a radio profile "default") #cap-reg-eirp 0
```

If DFS channels (shared with radar) are used on 802.11a/n radio, the following commands to alter the default radio profile or other defined radio profile will be necessary

```
(Aruba651) (802.11a radio-profile "default") #csa
```

```
(Aruba651) (802.11a radio-profile "default") #csa-count 4
```

```
(Aruba651) (802.11a radio-profile "default") #dot11h
```

### 2.4 GHz Radio settings

```
(Aruba651) (config) #rf dot11g-radio-profile default
```

Enable or disable 2.4 GHz radio

```
(Aruba651) (802.11g radio profile "default") #<no> radio-enable
```

Choose a channel

```
(Aruba651) (802.11g radio profile "default") #channel <desired channel>
```

Disable 40 MHz

```
(Aruba651) (802.11b radio profile "default") #<no> high-throughput enable
```



### Admin Tip: Transmit Power

For setting up the **Transmit Power**, please consult your facility's RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. Spectralink Wireless Telephones require the following minimum dBm reading to support the corresponding **Mandatory** data rate setting in the access point.

802.11 Radio Standard	Minimum Available Signal Strength (RSSI)	Maximum "Mandatory" Data Rate
802.11b	-65 dBm	11 Mb/s
802.11g	-67 dBm	6 Mb/s
802.11g	-47 dBm	54 Mb/s



### Web Info: RF Deployment reference

For additional details on RF deployment please see the *Deploying Enterprise-Grade Wi-Fi Telephony* White Paper.

```
(Aruba651) (802.11g radio profile "default")#tx-power <transmit EIRP in .5
dBm increments)
(Aruba651) (802.11g radio profile "default")#no spectrum-load-balancing
(Aruba651) (802.11g radio profile "default")#cap-reg-eirp 0
```

If using 8020/8030 phones or other devices that are not n-enabled

```
(Aruba651)# config terminal rf ht-radio-profile default-a
(Aruba651) (High-throughput radio profile "default-a") #CSD-override
(Aruba651)# exit
(Aruba651) (config)#rf ht-radio-profile default-g
(Aruba651) (High-throughput radio profile "default-g") #CSD-override
```

### Assigning the HT Radio Profiles to the Virtual AP

```
(Aruba651)# config terminal wlan virtual-ap spectralink-vap
(Aruba651) (Virtual AP profile "spectralink-vap") #configure terminal rf
ht-radio-profile default-g
(Aruba651) (Virtual AP profile "spectralink-vap") #configure terminal rf
ht-radio-profile default-a
```

### Creating an ARM profile

```
(Aruba 3600) #configure terminal rf arm-profile default
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default")
#assignment <disable or maintain >
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # voip-
aware-scan
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # 40MHz-
allowed All
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # client-
aware
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # no
active-scan
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # ota-
updates
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # scanning
```

```
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # multi-
band-scan
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # voip-
aware-scan
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # power-
save-aware scan
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # video-
aware-scan
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # no
client-match
(Aruba 3600) (Adaptive Radio Management (ARM) profile "default") # write
memory
```

## Assigning properties to an AP-Group

### Virtual AP assignment

```
(Aruba651) #configure terminal ap-group default
(Aruba651) (AP group "default") #virtual-ap spectralink-vap
(Aruba651) (AP group "default") #voip-cac-profile "8400_g"
(Aruba651) (AP group "default") #dot11a-traffic-mgmt-profile "AC_ON"
(Aruba651) (AP group "default") #dot11g-traffic-mgmt-profile "AC_ON"
```

Normally, one would have to assign the Radio-profile to an AP-Group. But this example uses the default radio profiles which are assigned to the default AP-Group automatically.

## On WebUI

### Creating a Virtual-AP

- 1 Navigate to **Configuration** and **AP Configuration**.
- 2 Click **Edit** against the default AP-Group.
- 3 Click **Wireless LAN** and **Virtual AP**.
- 4 Click **Add**.
- 5 On the right-pane, select **NEW** under **Add a profile** and enter a profile name (Ex., spectralink-vap) and click **Add**.
- 6 Click on the newly entered name and enter the following options
  - a Check **Virtual AP enable**.
  - b Allowed band – **all** (or select a band, if the design calls for voice on only one band).

- c Select the VLAN where the voice handsets and the Spectralink Gateway and Server would reside.
- d In the right pane, uncheck Convert Broadcast ARP requests to unicast.
- e Click **Apply**.

The screenshot shows the Aruba Spectralink VIEW configuration interface. The left sidebar contains a navigation menu with categories like WIZARDS, NETWORK, SECURITY, and WIRELESS. The main content area is titled 'Configuration > AP Group > Edit "default"'. It is divided into two panes: 'Profiles' on the left and 'Profile Details' on the right. The 'Profiles' pane shows a tree structure with 'Wireless LAN' expanded, containing 'Virtual AP', 'VPSK', 'spectralink-vap', 'AAA', '802.11K', 'Hotspot 2.0', 'SSID', 'WMM Traffic Management', 'ADYS', 'RF Management', 'AP', 'QOS', 'IDS', and 'Mesh'. The 'Profile Details' pane is for 'Virtual AP > spectralink-vap' and has tabs for 'Basic' and 'Advanced'. The 'Basic' tab is active, showing various configuration options with checkboxes, dropdown menus, and text input fields. At the bottom right of the configuration area is an 'Apply' button.

Profiles		Profile Details	
Wireless LAN		Virtual AP > spectralink-vap	
Virtual AP		Show Reference Save As Reset	
cac		Basic Advanced	
VPSK		Virtual AP enable <input checked="" type="checkbox"/>	
spectralink-vap		VLAN <input type="text"/>	
AAA spectralink-dot1x		Forward mode tunnel	
802.11K default		Allowed band all	
Hotspot 2.0 default		Band Steering <input type="checkbox"/>	
SSID view		Steering Mode prefer-5ghz	
WMM Traffic Management		Dynamic Multicast Optimization (DMO) <input type="checkbox"/>	
ADYS		Dynamic Multicast Optimization (DMO) Threshold 6	
RF Management		Drop Broadcast and Multicast <input type="checkbox"/>	
AP		Convert Broadcast ARP requests to unicast <input type="checkbox"/>	
QOS		Authentication Failure Blacklist Time 3600 sec	
IDS		Blacklist Time 3600 sec	
Mesh		Deny inter user traffic <input type="checkbox"/>	
		Deny time range --NONE--	
		DoS Prevention <input type="checkbox"/>	
		HA Discovery on-association <input checked="" type="checkbox"/>	
		Mobile IP <input checked="" type="checkbox"/>	
		Preserve Client VLAN <input type="checkbox"/>	
		QinQ Outer VLAN 0	
		Remote-AP Operation standard	
		Station Blacklisting <input checked="" type="checkbox"/>	
		Strict Compliance <input type="checkbox"/>	
		VLAN Mobility <input type="checkbox"/>	

## Creating a SSID-profile

- 1 Click the newly created virtual-ap in the left-hand Virtual AP list.
- 2 Click **SSID profile**.
  - a On the right pane, select **NEW** and enter an SSID-profile name (Ex., spectralink).
  - b Enter the desired SSID-name.
  - c When Spectralink phones are configured for None (not recommended, but useful for provisioning), under **Network Authentication**, select **None**, and under **Encryption**, select **Open**.
  - d When Spectralink phones are configured for WEP, under **Network Authentication**, select **None**, and under **Encryption**, select **WEP**. For the 40 Bits key on the Spectralink phone, use the 64-bit key Aruba setting, entering 10 hex digits. For the 104-bit key on the Spectralink phone, use the 128-bit key Aruba setting, entering 26 hex digits.

- e WPA-PSK is no longer available through the Web GUI. It must be entered with the following cli commands:

```
(Aruba651) #configure terminal wlan ssid-profile view
```

```
(Aruba651) (SSID Profile "view") #opmode wpa-psk-tkip
```

```
(Aruba651) (SSID Profile "view") #wpa-passphrase <"passphrase">
```

- f When Spectralink phones are configured for WPA2-PSK under **Network Authentication**, select **WPA2-PSK** and **AES** under **Encryption**. Enter a preshared key in either Hex or as a passphrase.
- g When Spectralink phones are configured for WPA2-Enterprise, under **Network Authentication** select **WPA2** and **AES** under **Encryption**.
- h Click **Apply**

**3** Click the **Advanced** tab on the right pane.

- a Make the following changes
- b **DTIM Interval – 2**
- c **802.11g transmit rates** – check **5, 6, 9, 11, 12, 18, 24, 36, 48, 54**.
- d **802.11g basic rates** – check **5, 11**
- e **802.11a transmit rates** – check, **6, 9, 12, 18, 24, 36, 48, 54**.
- f **802.11a basic rates** – check **6, 12, 24**
- g Uncheck **Wireless Multimedia (WMM)**.
- h Uncheck **Wireless Multimedia U-APSD (WMM-UAPSD) Powersave**
- i Check **Strict Spectralink Voice Protocol (SVP)**.
- j Ensure that **Maximum Transmit Failures** is 0.
- k Ensure that **Enable OKC** is checked.

**4** Click **Apply** and **Save Configuration**.

**ARUBA** networks MOBIILITY CONTROLLER | Aruba3600 [Log out adm](#)

Dashboard Monitoring **Configuration** Diagnostics Maintenance [Save Configuration](#)

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave  
 NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP  
 SECURITY  
 Authentication  
 Access Control  
 WIRELESS  
 > **AP Configuration**  
 AP Installation  
 MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold  
 ADVANCED SERVICES  
 Redundancy  
 AirGroup  
 IP Mobility  
 Stateful Firewall  
 External Services  
 VPN Services  
 Wired Access  
 All Profiles

**Configuration > AP Group > Edit "default"**

Profiles	Profile Details
<ul style="list-style-type: none"> <li>Wireless LAN               <ul style="list-style-type: none"> <li>Virtual AP                   <ul style="list-style-type: none"> <li>cac</li> <li>VPSK                       <ul style="list-style-type: none"> <li>AAA spectralink-aaa</li> <li>802.11K default</li> <li>Hotspot 2.0 default</li> <li>SSID view                           <ul style="list-style-type: none"> <li>EDCA Parameters Station AC_OFF</li> <li>EDCA Parameters AP AC_OFF</li> <li>High-throughput SSID default</li> <li>802.11r</li> <li>WMM Traffic Management</li> </ul> </li> </ul> </li> </ul> </li> <li>spectralink-vap                   <ul style="list-style-type: none"> <li>ADYS</li> </ul> </li> <li>RF Management                   <ul style="list-style-type: none"> <li>AP                       <ul style="list-style-type: none"> <li>QoS</li> <li>IDS</li> <li>Mesh</li> </ul> </li> </ul> </li> </ul> </li> </ul>	<p>SSID Profile &gt; view <a href="#">Show Reference</a> <a href="#">Save As</a> <a href="#">Reset</a></p> <p>Basic Advanced</p> <p>SSID enable <input checked="" type="checkbox"/></p> <p>ESSID view</p> <p>Encryption           <ul style="list-style-type: none"> <li><input type="checkbox"/> opensystem <input type="checkbox"/> static-wep</li> <li><input type="checkbox"/> dynamic-wep</li> <li><input type="checkbox"/> wpa-tkip <input type="checkbox"/> wpa-aes</li> <li><input type="checkbox"/> wpa-psk-tkip</li> <li><input type="checkbox"/> wpa-psk-aes</li> <li><input checked="" type="checkbox"/> wpa2-aes <input type="checkbox"/> wpa2-psk-aes</li> <li><input type="checkbox"/> wpa2-psk-tkip</li> <li><input type="checkbox"/> wpa2-tkip</li> </ul> </p> <p>DTIM Interval 2 beacon periods</p> <p>802.11a Basic Rates           <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> 6 <input type="checkbox"/> 9 <input checked="" type="checkbox"/> 12 <input type="checkbox"/> 18 <input checked="" type="checkbox"/> 24</li> <li><input type="checkbox"/> 36 <input type="checkbox"/> 48 <input type="checkbox"/> 54</li> </ul> </p> <p>802.11a Transmit Rates           <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 12 <input checked="" type="checkbox"/> 18 <input checked="" type="checkbox"/> 24</li> <li><input checked="" type="checkbox"/> 36 <input checked="" type="checkbox"/> 48 <input checked="" type="checkbox"/> 54</li> </ul> </p> <p>802.11g Basic Rates           <ul style="list-style-type: none"> <li><input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 5 <input type="checkbox"/> 6 <input type="checkbox"/> 9 <input checked="" type="checkbox"/> 11</li> <li><input type="checkbox"/> 12 <input type="checkbox"/> 18 <input type="checkbox"/> 24 <input type="checkbox"/> 36</li> <li><input type="checkbox"/> 48 <input type="checkbox"/> 54</li> </ul> </p> <p>802.11g Transmit Rates           <ul style="list-style-type: none"> <li><input type="checkbox"/> 1 <input type="checkbox"/> 2 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> 6 <input checked="" type="checkbox"/> 9 <input checked="" type="checkbox"/> 11</li> <li><input checked="" type="checkbox"/> 12 <input checked="" type="checkbox"/> 18 <input checked="" type="checkbox"/> 24 <input checked="" type="checkbox"/> 36</li> <li><input checked="" type="checkbox"/> 48 <input checked="" type="checkbox"/> 54</li> </ul> </p> <p>Station Ageout Time 1000 sec</p> <p>Max Transmit Attempts 8</p> <p>RTS Threshold 2333 bytes</p> <p>Short Preamble <input checked="" type="checkbox"/></p> <p>Max Associations 64</p> <p>Wireless Multimedia (WMM) <input type="checkbox"/></p> <p><a href="#">Apply</a></p>

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
AP  
Controller  
Campus WLAN  
Remote AP  
AirWave

NETWORK  
Controller  
VLANs  
Ports  
Cellular Profile  
IP

SECURITY  
Authentication  
Access Control

WIRELESS  
AP Configuration  
AP Installation  
MANAGEMENT  
General  
Administration  
Certificates  
SNMP  
Logging  
Clock  
Guest Provisioning  
Captive Portal  
SMTP  
Bandwidth Calculator  
Threshold

ADVANCED SERVICES  
Redundancy  
AirGroup  
IP Mobility  
Stateful Firewall  
External Services  
VPN Services  
Wired Access  
All Profiles

**Configuration > AP Group > Edit "default"**

Profiles	Profile Details
<input checked="" type="checkbox"/> Wireless LAN	
<input checked="" type="checkbox"/> Virtual AP	
<input checked="" type="checkbox"/> cac	
<input checked="" type="checkbox"/> VPSK	
<input checked="" type="checkbox"/> AAA	spectralink-aaa
<input checked="" type="checkbox"/> 802.11K	default
<input checked="" type="checkbox"/> Hotspot 2.0	default
<input checked="" type="checkbox"/> SSID	view
<input checked="" type="checkbox"/> EDCA Parameters Station	AC_OFF
<input checked="" type="checkbox"/> EDCA Parameters AP	AC_OFF
<input checked="" type="checkbox"/> High-throughput SSID	default
<input checked="" type="checkbox"/> 802.11r	
<input checked="" type="checkbox"/> WMM Traffic Management	
<input checked="" type="checkbox"/> spectralink-vap	
<input checked="" type="checkbox"/> ADYS	
<input checked="" type="checkbox"/> RF Management	
<input checked="" type="checkbox"/> AP	
<input checked="" type="checkbox"/> QoS	
<input checked="" type="checkbox"/> IDS	
<input checked="" type="checkbox"/> Mesh	

Wireless Multimedia (WMM)	<input type="checkbox"/>
Wireless Multimedia U-APSD (WMM-UAPSD)	<input type="checkbox"/>
Powersave	<input type="checkbox"/>
WMM TSPEC Min Inactivity Interval	0 msec
Override DSCP mappings for WMM clients	<input type="checkbox"/>
DSCP mapping for WMM voice AC	46
DSCP mapping for WMM video AC	40
DSCP mapping for WMM best-effort AC	0
DSCP mapping for WMM background AC	0
Multiple Tx Replay Counters	<input type="checkbox"/>
Hide SSID	<input type="checkbox"/>
Deny_Broadcast Probes	<input type="checkbox"/>
Local Probe Request Threshold (dB)	0
Disable Probe Retry	<input checked="" type="checkbox"/>
Battery Boost	<input type="checkbox"/>
WEP Key 1	Retype:
WEP Key 2	Retype:
WEP Key 3	Retype:
WEP Key 4	Retype:
WEP Transmit Key Index	1
WPA Hexkey	Retype:
WPA Passphrase	Retype:

Specify static WEP key 4 of 4 (length 10 or 26 Hex characters).

Anniv

Dashboard | Monitoring | **Configuration** | Diagnostics | Maintenance | Save Configuration

WIZARDS

- AP
- Controller
- Campus WLAN
- Remote AP
- AirWave

NETWORK

- Controller
- VLANs
- Ports
- Cellular Profile
- IP

SECURITY

- Authentication
- Access Control

WIRELESS

- > **AP Configuration**
  - AP Installation

MANAGEMENT

- General
- Administration
- Certificates
- SNMP
- Logging
- Clock
- Guest Provisioning
- Captive Portal
- SMTP
- Bandwidth Calculator
- Threshold

**Configuration > AP Group > Edit "default"**

Profiles	Profile Details
<ul style="list-style-type: none"> <li>Wireless LAN               <ul style="list-style-type: none"> <li>Virtual AP                   <ul style="list-style-type: none"> <li>ADYS                       <ul style="list-style-type: none"> <li>AAA <span>spectralink-aaa</span> <ul style="list-style-type: none"> <li>802.11K <span>default</span> <ul style="list-style-type: none"> <li>Hotspot 2.0                           <ul style="list-style-type: none"> <li>SSID <span>ADYARUBA</span> <ul style="list-style-type: none"> <li>EDCA Parameters Station <span>AC_OFF</span></li> <li>EDCA Parameters AP <span>AC_OFF</span></li> <li>High-throughput SSID <span>ht-enable_20</span></li> <li>802.11r</li> <li>WMM Traffic Management</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> <li>RF Management               <ul style="list-style-type: none"> <li>AP                   <ul style="list-style-type: none"> <li>QOS</li> <li>IDS</li> <li>Mesh</li> </ul> </li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>WEP Key 3 <span>Retype:</span></li> <li>WEP Key 4 <span>Retype:</span></li> <li>WEP Transmit Key Index <span>1</span></li> <li>WPA Hexkey <span>Retype:</span></li> <li>WPA Passphrase <span>Retype:</span></li> <li>Maximum Transmit Failures <span>0</span></li> <li>BC/MC Rate Optimization <input type="checkbox"/></li> <li>Rate Optimization for delivering EAPOL frames <input checked="" type="checkbox"/></li> <li>Strict Spectralink Voice Protocol (SVP) <input type="checkbox"/></li> <li>802.11g Beacon Rate <span>default</span></li> <li>802.11a Beacon Rate <span>default</span></li> <li>Video Multicast Rate Optimization <span>default</span></li> <li>Advertise QBSS Load IE <input checked="" type="checkbox"/></li> <li>Advertise Location Info <input type="checkbox"/></li> <li>Advertise AP Name <input type="checkbox"/></li> <li>Enforce user vlan for open stations <input type="checkbox"/></li> <li>Enable OKC <input checked="" type="checkbox"/></li> </ul>

## Creating a High-Throughput SSID profile for an 802.11n-disabled network

- 1 Click **High-Throughput SSID Profile**.
- 2 Drop down on the right-pane and select **NEW**. Provide name (Ex., ht-disabled).
- 3 Modify the following
  - a Uncheck **High-Throughput enable**.
- 4 Click **Apply**.
- 5 Click **Save Configuration**.



Dashboard | Monitoring | **Configuration** | Diagnostics | Maintenance | Save Configuration

WIZARDS  
AP  
Controller  
Campus WLAN  
Remote AP  
AirWave

NETWORK  
Controller  
VLANs  
Ports  
Cellular Profile  
IP

SECURITY  
Authentication  
Access Control

WIRELESS  
AP Configuration  
AP Installation

MANAGEMENT  
General  
Administration  
Certificates  
SNMP  
Logging  
Clock  
Guest Provisioning  
Captive Portal  
SMTP  
Bandwidth Calculator  
Threshold

ADVANCED SERVICES  
Redundancy  
AirGroup  
IP Mobility  
Stateful Firewall  
External Services  
VPN Services  
Wired Access  
All Profiles

**Configuration > AP Group > Edit "default"**

Profiles	Profile Details																																																				
<ul style="list-style-type: none"> <li>Wireless LAN               <ul style="list-style-type: none"> <li>Virtual AP                   <ul style="list-style-type: none"> <li>cac</li> <li>VPSK                       <ul style="list-style-type: none"> <li>AAA: spectralink-aaa</li> <li>802.11K: default</li> <li>Hotspot 2.0: default</li> <li>SSID: VPSK                           <ul style="list-style-type: none"> <li>EDCA Parameters Station: AC_OFF</li> <li>EDCA Parameters AP: AC_OFF</li> <li><b>High-throughput SSID: ht-disable</b></li> <li>802.11r</li> <li>WMM Traffic Management</li> </ul> </li> </ul> </li> </ul> </li> <li>spectralink-vap                   <ul style="list-style-type: none"> <li>ADYS</li> <li>RF Management                       <ul style="list-style-type: none"> <li>AP                           <ul style="list-style-type: none"> <li>QOS</li> <li>IDS</li> <li>Mesh</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul>	<p><b>High-throughput SSID Profile &gt;</b> ht-disable <span>Show Reference</span> <span>Save As</span> <span>Reset</span></p> <p>Basic   <b>Advanced</b></p> <table border="1"> <tr><td>High throughput enable (SSID)</td><td><input type="checkbox"/></td></tr> <tr><td>40 MHz channel usage</td><td><input type="checkbox"/></td></tr> <tr><td>Very High throughput enable (SSID)</td><td><input type="checkbox"/></td></tr> <tr><td>80 MHz channel usage (VHT)</td><td><input type="checkbox"/></td></tr> <tr><td>BA AMSDU Enable</td><td><input type="checkbox"/></td></tr> <tr><td>Temporal Diversity Enable</td><td><input type="checkbox"/></td></tr> <tr><td>Legacy stations</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Low-density Parity Check</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Maximum number of spatial streams usable for STBC reception</td><td>1</td></tr> <tr><td>Maximum number of spatial streams usable for STBC transmission</td><td>1</td></tr> <tr><td>MPDU Aggregation</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Max received A-MPDU size</td><td>65535</td></tr> <tr><td>Max transmitted A-MPDU size</td><td>65535 bytes</td></tr> <tr><td>Min MPDU start spacing</td><td>0</td></tr> <tr><td>Short guard interval in 20 MHz mode</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Short guard interval in 40 MHz mode</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Short guard interval in 80 MHz mode</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Supported MCS set</td><td>0-23</td></tr> <tr><td>VHT - Supported MCS map</td><td>9 9 9 9</td></tr> <tr><td>VHT - Explicit Transmit Beamforming</td><td><input type="checkbox"/></td></tr> <tr><td>VHT - Transmit Beamforming Sounding Interval</td><td>25 msec</td></tr> <tr><td>Maximum VHT MPDU size</td><td>11454</td></tr> <tr><td>Maximum number of MSDUs in an A-MSDU on best-effort AC</td><td>10 MSDUs</td></tr> <tr><td>Maximum number of MSDUs in an A-MSDU on background AC</td><td>10 MSDUs</td></tr> <tr><td>Maximum number of MSDUs in an A-MSDU on video AC</td><td>3 MSDUs</td></tr> <tr><td>Maximum number of MSDUs in an A-MSDU on voice AC</td><td>3 MSDUs</td></tr> </table> <p><span>Configuration Updated Successfully.</span> <span>Apply</span></p>	High throughput enable (SSID)	<input type="checkbox"/>	40 MHz channel usage	<input type="checkbox"/>	Very High throughput enable (SSID)	<input type="checkbox"/>	80 MHz channel usage (VHT)	<input type="checkbox"/>	BA AMSDU Enable	<input type="checkbox"/>	Temporal Diversity Enable	<input type="checkbox"/>	Legacy stations	<input checked="" type="checkbox"/>	Low-density Parity Check	<input checked="" type="checkbox"/>	Maximum number of spatial streams usable for STBC reception	1	Maximum number of spatial streams usable for STBC transmission	1	MPDU Aggregation	<input checked="" type="checkbox"/>	Max received A-MPDU size	65535	Max transmitted A-MPDU size	65535 bytes	Min MPDU start spacing	0	Short guard interval in 20 MHz mode	<input checked="" type="checkbox"/>	Short guard interval in 40 MHz mode	<input checked="" type="checkbox"/>	Short guard interval in 80 MHz mode	<input checked="" type="checkbox"/>	Supported MCS set	0-23	VHT - Supported MCS map	9 9 9 9	VHT - Explicit Transmit Beamforming	<input type="checkbox"/>	VHT - Transmit Beamforming Sounding Interval	25 msec	Maximum VHT MPDU size	11454	Maximum number of MSDUs in an A-MSDU on best-effort AC	10 MSDUs	Maximum number of MSDUs in an A-MSDU on background AC	10 MSDUs	Maximum number of MSDUs in an A-MSDU on video AC	3 MSDUs	Maximum number of MSDUs in an A-MSDU on voice AC	3 MSDUs
High throughput enable (SSID)	<input type="checkbox"/>																																																				
40 MHz channel usage	<input type="checkbox"/>																																																				
Very High throughput enable (SSID)	<input type="checkbox"/>																																																				
80 MHz channel usage (VHT)	<input type="checkbox"/>																																																				
BA AMSDU Enable	<input type="checkbox"/>																																																				
Temporal Diversity Enable	<input type="checkbox"/>																																																				
Legacy stations	<input checked="" type="checkbox"/>																																																				
Low-density Parity Check	<input checked="" type="checkbox"/>																																																				
Maximum number of spatial streams usable for STBC reception	1																																																				
Maximum number of spatial streams usable for STBC transmission	1																																																				
MPDU Aggregation	<input checked="" type="checkbox"/>																																																				
Max received A-MPDU size	65535																																																				
Max transmitted A-MPDU size	65535 bytes																																																				
Min MPDU start spacing	0																																																				
Short guard interval in 20 MHz mode	<input checked="" type="checkbox"/>																																																				
Short guard interval in 40 MHz mode	<input checked="" type="checkbox"/>																																																				
Short guard interval in 80 MHz mode	<input checked="" type="checkbox"/>																																																				
Supported MCS set	0-23																																																				
VHT - Supported MCS map	9 9 9 9																																																				
VHT - Explicit Transmit Beamforming	<input type="checkbox"/>																																																				
VHT - Transmit Beamforming Sounding Interval	25 msec																																																				
Maximum VHT MPDU size	11454																																																				
Maximum number of MSDUs in an A-MSDU on best-effort AC	10 MSDUs																																																				
Maximum number of MSDUs in an A-MSDU on background AC	10 MSDUs																																																				
Maximum number of MSDUs in an A-MSDU on video AC	3 MSDUs																																																				
Maximum number of MSDUs in an A-MSDU on voice AC	3 MSDUs																																																				

## Creating a High-Throughput SSID profile for an 802.11n-enabled network

- 1 Click **High-Throughput SSID Profile**.
- 2 On the right pane, click on the **Advanced** tab.
- 3 Drop down on the right-pane and select **NEW**. Provide name (Ex., ht-enable-80).
- 4 Modify the following
  - a Check **High-Throughput enable**.
  - b Check **40 MHz channel usage** or uncheck for 20 MHz usage.
  - c Check **Very High throughput enable (SSID)** and **80 MHz channel usage (VHT)** for 80 MHz channel usage. Note: the AP must be power cycled for the 80 MHz setting to take effect.



### Admin Tip: Paired channel recommendation

40 MHz (paired) channels are not recommended by Aruba on the 2.4 GHz radio band.

**Admin Tip: Paired channel recommendation**

40 MHz (paired) channels are not recommended by Aruba on the 2.4 GHz radio band.

- d Ensure that Temporal Diversity Enable is unchecked.
- e Check **MPDU Aggregation**.
- f Check **Legacy Stations**.
- g Check Short guard interval in 20 MHz mode.
- h Check Short guard interval in 40 MHz mode.
- i For 12x and 13x AP's, set the **Maximum number of MSDUs in an A-MSDU on best-effort AC** and the **Maximum number of MSDU's in an A-MSDU on background AC** both to 10. For 11n AP's with model numbers smaller than 12x, set these values to 3.
- j Set the **Maximum number of MSDUs in an A-MSDU on video AC** and **Maximum number of MSDUs in an A-MSDU on voice AC** both to 3.

**Admin Tip: A-MSDU Aggregation Settings**

The AP-125 and AP-135 and newer AP's can process 10 packets per background and best effort aggregation. Older 11n AP's have better performance with a setting of 3 packets per background and best effort aggregation. Voice and video should remain with 3 packets per aggregation to avoid audible/visible latency issues.

- 5 Click **Apply**.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave  
 NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP  
 SECURITY  
 Authentication  
 Access Control  
 WIRELESS  
 > **AP Configuration**  
 AP Installation  
 MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold  
 ADVANCED SERVICES  
 Redundancy  
 AirGroup  
 IP Mobility  
 Stateful Firewall  
 External Services  
 VPN Services  
 Wired Access  
 All Profiles

**Configuration > AP Group > Edit "default"**

Profiles	Profile Details																																																				
<ul style="list-style-type: none"> <li>Wireless LAN               <ul style="list-style-type: none"> <li>Virtual AP                   <ul style="list-style-type: none"> <li>cac</li> <li>VPSK</li> <li>spectralink-vap</li> <li>AAA                       <ul style="list-style-type: none"> <li>spectralink-dot1x</li> <li>802.11K                           <ul style="list-style-type: none"> <li>default</li> <li>Hotspot 2.0                               <ul style="list-style-type: none"> <li>default</li> <li>SSID                                   <ul style="list-style-type: none"> <li>view</li> <li>EDCA Parameters Station                                       <ul style="list-style-type: none"> <li>AC_OFF</li> <li>EDCA Parameters AP   <ul style="list-style-type: none"> <li>AC_OFF</li> <li>High-throughput SSID   <ul style="list-style-type: none"> <li>ht_enable_80</li> <li>802.11r</li> <li>WMM Traffic Management</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> </ul> </li> <li>ADYS                   <ul style="list-style-type: none"> <li>RF Management                       <ul style="list-style-type: none"> <li>AP</li> <li>QOS</li> <li>IDS</li> <li>Mesh</li> </ul> </li> </ul> </li> </ul> </li> </ul> </li></ul></li></ul>	<p><b>High-throughput SSID Profile &gt;</b> ht_enable_80 Show Reference Save As Reset</p> <p>Basic Advanced</p> <table border="1"> <tbody> <tr><td>High throughput enable (SSID)</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>40 MHz channel usage</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Very High throughput enable (SSID)</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>80 MHz channel usage (VHT)</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>BA AMSDU Enable</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Temporal Diversity Enable</td><td><input type="checkbox"/></td></tr> <tr><td>Legacy stations</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Low-density Parity Check</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Maximum number of spatial streams usable for STBC reception</td><td>1</td></tr> <tr><td>Maximum number of spatial streams usable for STBC transmission</td><td>1</td></tr> <tr><td>MPDU Aggregation</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Max received A-MPDU size</td><td>65535</td></tr> <tr><td>Max transmitted A-MPDU size</td><td>65535 bytes</td></tr> <tr><td>Min MPDU start spacing</td><td>0</td></tr> <tr><td>Short guard interval in 20 MHz mode</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Short guard interval in 40 MHz mode</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>Short guard interval in 80 MHz mode</td><td><input type="checkbox"/></td></tr> <tr><td>Supported MCS set</td><td>0-23 &lt;-- &gt;</td></tr> <tr><td>VHT - Supported MCS map</td><td>9 9 9 9</td></tr> <tr><td>VHT - Explicit Transmit Beamforming</td><td><input checked="" type="checkbox"/></td></tr> <tr><td>VHT - Transmit Beamforming Sounding Interval</td><td>25 msec</td></tr> <tr><td>Maximum VHT MPDU size</td><td>11454</td></tr> <tr><td>Maximum number of MSDUs in an A-MSDU on best-effort AC</td><td>10 MSDUs</td></tr> <tr><td>Maximum number of MSDUs in an A-MSDU on background AC</td><td>10 MSDUs</td></tr> <tr><td>Maximum number of MSDUs in an A-MSDU on video AC</td><td>3 MSDUs</td></tr> <tr><td>Maximum number of MSDUs in an A-MSDU on voice AC</td><td>3 MSDUs</td></tr> </tbody> </table>	High throughput enable (SSID)	<input checked="" type="checkbox"/>	40 MHz channel usage	<input checked="" type="checkbox"/>	Very High throughput enable (SSID)	<input checked="" type="checkbox"/>	80 MHz channel usage (VHT)	<input checked="" type="checkbox"/>	BA AMSDU Enable	<input checked="" type="checkbox"/>	Temporal Diversity Enable	<input type="checkbox"/>	Legacy stations	<input checked="" type="checkbox"/>	Low-density Parity Check	<input checked="" type="checkbox"/>	Maximum number of spatial streams usable for STBC reception	1	Maximum number of spatial streams usable for STBC transmission	1	MPDU Aggregation	<input checked="" type="checkbox"/>	Max received A-MPDU size	65535	Max transmitted A-MPDU size	65535 bytes	Min MPDU start spacing	0	Short guard interval in 20 MHz mode	<input checked="" type="checkbox"/>	Short guard interval in 40 MHz mode	<input checked="" type="checkbox"/>	Short guard interval in 80 MHz mode	<input type="checkbox"/>	Supported MCS set	0-23 <-- >	VHT - Supported MCS map	9 9 9 9	VHT - Explicit Transmit Beamforming	<input checked="" type="checkbox"/>	VHT - Transmit Beamforming Sounding Interval	25 msec	Maximum VHT MPDU size	11454	Maximum number of MSDUs in an A-MSDU on best-effort AC	10 MSDUs	Maximum number of MSDUs in an A-MSDU on background AC	10 MSDUs	Maximum number of MSDUs in an A-MSDU on video AC	3 MSDUs	Maximum number of MSDUs in an A-MSDU on voice AC	3 MSDUs
High throughput enable (SSID)	<input checked="" type="checkbox"/>																																																				
40 MHz channel usage	<input checked="" type="checkbox"/>																																																				
Very High throughput enable (SSID)	<input checked="" type="checkbox"/>																																																				
80 MHz channel usage (VHT)	<input checked="" type="checkbox"/>																																																				
BA AMSDU Enable	<input checked="" type="checkbox"/>																																																				
Temporal Diversity Enable	<input type="checkbox"/>																																																				
Legacy stations	<input checked="" type="checkbox"/>																																																				
Low-density Parity Check	<input checked="" type="checkbox"/>																																																				
Maximum number of spatial streams usable for STBC reception	1																																																				
Maximum number of spatial streams usable for STBC transmission	1																																																				
MPDU Aggregation	<input checked="" type="checkbox"/>																																																				
Max received A-MPDU size	65535																																																				
Max transmitted A-MPDU size	65535 bytes																																																				
Min MPDU start spacing	0																																																				
Short guard interval in 20 MHz mode	<input checked="" type="checkbox"/>																																																				
Short guard interval in 40 MHz mode	<input checked="" type="checkbox"/>																																																				
Short guard interval in 80 MHz mode	<input type="checkbox"/>																																																				
Supported MCS set	0-23 <-- >																																																				
VHT - Supported MCS map	9 9 9 9																																																				
VHT - Explicit Transmit Beamforming	<input checked="" type="checkbox"/>																																																				
VHT - Transmit Beamforming Sounding Interval	25 msec																																																				
Maximum VHT MPDU size	11454																																																				
Maximum number of MSDUs in an A-MSDU on best-effort AC	10 MSDUs																																																				
Maximum number of MSDUs in an A-MSDU on background AC	10 MSDUs																																																				
Maximum number of MSDUs in an A-MSDU on video AC	3 MSDUs																																																				
Maximum number of MSDUs in an A-MSDU on voice AC	3 MSDUs																																																				

## 6 Click **Save Configuration**.

### Assigning an AAA-profile

- 1 Click **AAA Profile** on the middle pane and select the AAA profile created for the voice devices (spectralink-aaa for non-enterprise security or spectralink-dot1x for enterprise security).
- 2 Click **Apply** and **Save Configuration**.

Dashboard
Monitoring
Configuration
Diagnostics
Maintenance
Save Configuration

WIZARDS
AP
Controller
Campus WLAN
Remote AP
AirWave
NETWORK
Controller
VLANs
Ports
Cellular Profile
IP
SECURITY
Authentication
Access Control
WIRELESS
AP Configuration
AP Installation
MANAGEMENT
General
Administration
Certificates
SNMP
Logging
Clock
Guest Provisioning
Captve Portal
SMTP
Bandwidth Calculator
Threshold
ADVANCED SERVICES
Redundancy
AirGroup
IP Mobility
Stateful Firewall
External Services
VPN Services
Wired Access
All Profiles

## Configuration > AP Group > Edit "default"

Profiles	Profile Details																																				
<div>Wireless LAN</div> <div>Virtual AP</div> <div> cac VPSK spectralink-vap </div> <div> <div>AAA</div> spectralink-dot1x </div> <div> <div>802.11K</div> default </div> <div> <div>Hotspot 2.0</div> default </div> <div> <div>SSID</div> view </div> <div> <div>EDCA Parameters Station</div> AC_OFF </div> <div> <div>EDCA Parameters AP</div> AC_OFF </div> <div> <div>High-throughput SSID</div> default </div> <div> <div>802.11r</div> </div> <div> <div>WMM Traffic Management</div> </div> <div> <div>ADYS</div> </div> <div> <div>RF Management</div> </div> <div> <div>AP</div> </div> <div> <div>QOS</div> </div> <div> <div>IDS</div> </div> <div> <div>Mesh</div> </div>	<div> <div>AAA Profile &gt;</div> spectralink-dot1x <div>Show Reference</div> </div> <table> <tr> <td>Initial role</td> <td>logon</td> </tr> <tr> <td>MAC Authentication Default Role</td> <td>guest</td> </tr> <tr> <td>802.1X Authentication Default Role</td> <td>guest</td> </tr> <tr> <td>L2 Authentication Fail Through</td> <td><input type="checkbox"/></td> </tr> <tr> <td>User idle timeout</td> <td> <input type="checkbox"/> Enable seconds </td> </tr> <tr> <td>RADIUS Interim Accounting</td> <td><input type="checkbox"/></td> </tr> <tr> <td>User derivation rules</td> <td>spectralink-derivation</td> </tr> <tr> <td>Wired to Wireless Roaming</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>SIP authentication role</td> <td>--NONE--</td> </tr> <tr> <td>Device Type Classification</td> <td><input checked="" type="checkbox"/></td> </tr> <tr> <td>Enforce DHCP</td> <td><input type="checkbox"/></td> </tr> <tr> <td>MAC Authentication Profile</td> <td></td> </tr> <tr> <td>MAC Authentication Server Group</td> <td>default</td> </tr> <tr> <td>802.1X Authentication Profile</td> <td>spectralink-802.1x</td> </tr> <tr> <td>802.1X Authentication Server Group</td> <td>RADIUS</td> </tr> <tr> <td>RADIUS Accounting Server Group</td> <td></td> </tr> <tr> <td>XML API server</td> <td></td> </tr> <tr> <td>RFC 3576 server</td> <td></td> </tr> </table>	Initial role	logon	MAC Authentication Default Role	guest	802.1X Authentication Default Role	guest	L2 Authentication Fail Through	<input type="checkbox"/>	User idle timeout	<input type="checkbox"/> Enable seconds	RADIUS Interim Accounting	<input type="checkbox"/>	User derivation rules	spectralink-derivation	Wired to Wireless Roaming	<input checked="" type="checkbox"/>	SIP authentication role	--NONE--	Device Type Classification	<input checked="" type="checkbox"/>	Enforce DHCP	<input type="checkbox"/>	MAC Authentication Profile		MAC Authentication Server Group	default	802.1X Authentication Profile	spectralink-802.1x	802.1X Authentication Server Group	RADIUS	RADIUS Accounting Server Group		XML API server		RFC 3576 server	
Initial role	logon																																				
MAC Authentication Default Role	guest																																				
802.1X Authentication Default Role	guest																																				
L2 Authentication Fail Through	<input type="checkbox"/>																																				
User idle timeout	<input type="checkbox"/> Enable seconds																																				
RADIUS Interim Accounting	<input type="checkbox"/>																																				
User derivation rules	spectralink-derivation																																				
Wired to Wireless Roaming	<input checked="" type="checkbox"/>																																				
SIP authentication role	--NONE--																																				
Device Type Classification	<input checked="" type="checkbox"/>																																				
Enforce DHCP	<input type="checkbox"/>																																				
MAC Authentication Profile																																					
MAC Authentication Server Group	default																																				
802.1X Authentication Profile	spectralink-802.1x																																				
802.1X Authentication Server Group	RADIUS																																				
RADIUS Accounting Server Group																																					
XML API server																																					
RFC 3576 server																																					

## Assigning a 5 GHz Radio-profile

- 1 Click **RF Management** under the **Virtual AP**.
- 2 Click **802.11a radio-profile**.
- 3 Click the **Advanced** tab.
  - a Click **Radio enable** to turn the 802.11a radio on.
  - b In the default profile on the right-pane, enter a 5 GHz channel.
  - c Clear or set the High throughput enable (radio) according to whether the radio is 802.11n-enabled mode or not.
  - d Choose a **Transmit EIRP** chosen to support the site survey plan and the maximum mandatory data rate as described immediately below.



### Admin Tip: Transmit Power

For setting up the **Transmit Power**, please consult your facility's RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. Spectralink Wireless Telephones require the following minimum dBm reading to support the corresponding **Mandatory** data rate setting in the access point.

<i>802.11 Radio Standard</i>	<i>Minimum Available Signal Strength (RSSI)</i>	<i>Maximum "Mandatory" Data Rate</i>
802.11a	-60 dBm	6 Mb/s
	-45 dBm	54 Mb/s



### Web Info: RF Deployment reference

For additional details on RF deployment please see the *Deploying Enterprise-Grade Wi-Fi Telephony* White Paper.

- e If DFS channels are to be used (channels shared with radar applications)
    - a. Click **Advertise 802.11d and 802.11h Capabilities**
    - b. Click **Enable CSA**
    - c. Set **CSA Count** to 4.
  - f Ensure that **Spectrum Load Balancing** is unchecked.
  - g Ensure that **Advertised regulatory max EIRP** is 0.
- 4 Click **Apply**.
- a Ensure that **Spectrum Load Balancing** is unchecked.
  - b Ensure that **Advertised regulatory max EIRP** is 0.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave

NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP

SECURITY  
 Authentication  
 Access Control

WIRELESS  
 > **AP Configuration**  
 AP Installation

MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold

ADVANCED SERVICES  
 Redundancy  
 AirGroup  
 IP Mobility  
 Stateful Firewall  
 External Services  
 VPN Services  
 Wired Access  
 All Profiles

**Configuration > AP Group > Edit "default"**

Profiles	Profile Details
<input type="checkbox"/> Wireless LAN <input type="checkbox"/> Virtual AP <input type="checkbox"/> RF Management <input checked="" type="checkbox"/> <b>802.11a radio</b> default Adaptive Radio Management (ARM) default High-throughput Radio default-a AM Scanning default <input checked="" type="checkbox"/> 802.11g radio default RF Optimization default RF Event Thresholds default <input checked="" type="checkbox"/> AP <input checked="" type="checkbox"/> QOS <input checked="" type="checkbox"/> IDS <input checked="" type="checkbox"/> Mesh	<b>802.11a radio profile &gt; default</b> Show Reference Save As Reset Basic Advanced Radio enable <input checked="" type="checkbox"/> Mode ap-mode High throughput enable (radio) <input checked="" type="checkbox"/> Very high throughput enable (radio) <input checked="" type="checkbox"/> Channel 149 Channel Width: <input type="radio"/> 20MHz <input type="radio"/> 40MHz <input checked="" type="radio"/> 80MHz Transmit EIRP 3 Non-Wi-Fi Interference Immunity 2 Enable CSA <input checked="" type="checkbox"/> CSA Count 4 Advertise 802.11d and 802.11h Capabilities <input checked="" type="checkbox"/> Spectrum Load Balancing <input type="checkbox"/> Beacon Period 100 msec Beacon Regulate <input type="checkbox"/> Advertized regulatory max EIRP 0 ARM/WIDS Override OFF Reduce Cell Size (Rx Sensitivity) 0 dB Management Frame Throttle interval 1 sec Management Frame Throttle Limit 20 Maximum Distance 0 meters RX Sensitivity Threshold 0 dB RX Sensitivity Tuning Based Channel Reuse disable

Commands Apply View Commands

- 5 Click **Adaptive Radio Management (ARM)** profile.
- 6 Modify the settings as follows
  - a Ensure that Assignment is set to disable or maintain.
  - b Set Allowed bands for 40MHz channels to a-only.
  - c Check **Client Aware**.
  - d Ensure that **Active Scan** is not checked.
  - e Ensure that ARM Over the Air Updates, Scanning, Multi Band Scan, VoIP Aware Scan, Power Save Aware Scan, and Video Aware Scan are checked.
  - f Ensure that **Client Match** is NOT checked.
- 7 Click **Apply** and **Save Configuration**.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave  
 NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP  
 SECURITY  
 Authentication  
 Access Control  
 WIRELESS  
 > **AP Configuration**  
 AP Installation  
 MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold  
 ADVANCED SERVICES  
 Redundancy  
 AirGroup  
 IP Mobility  
 Stateful Firewall  
 External Services  
 VPN Services  
 Wired Access  
 All Profiles

**Configuration > AP Group > Edit "default"**

Profiles		Profile Details	
<input type="checkbox"/> Wireless LAN			
<input checked="" type="checkbox"/> Virtual AP			
<input type="checkbox"/> RF Management			
<input checked="" type="checkbox"/> 802.11a radio	default		
<a href="#">Adaptive Radio Management (ARM)</a>	default		
High-throughput Radio	default-a		
AM Scanning	default		
<input checked="" type="checkbox"/> 802.11g radio	default		
RF Optimization	default		
RF Event Thresholds	default		
<input checked="" type="checkbox"/> AP			
<input checked="" type="checkbox"/> QOS			
<input checked="" type="checkbox"/> IDS			
<input checked="" type="checkbox"/> Mesh			

Profile Details	
Basic	Advanced
Assignment	disable
Allowed bands for 40MHz channels	a-only
80MHz support	<input checked="" type="checkbox"/>
Client Aware	<input checked="" type="checkbox"/>
Max Tx EIRP	127
Min Tx EIRP	9
Rogue AP Aware	<input type="checkbox"/>
Active Scan	<input type="checkbox"/>
ARM Over the Air Updates	<input checked="" type="checkbox"/>
Scanning	<input checked="" type="checkbox"/>
Multi Band Scan	<input checked="" type="checkbox"/>
VoIP Aware Scan	<input checked="" type="checkbox"/>
Power Save Aware Scan	<input checked="" type="checkbox"/>
Video Aware Scan	<input checked="" type="checkbox"/>
Ideal Coverage Index	10
Acceptable Coverage Index	4
Free Channel Index	25
Backoff Time	240 sec
Error Rate Threshold	50 %
Error Rate Wait Time	30 sec
Channel Quality Aware Arm	<input type="checkbox"/>
Channel Quality Threshold	70 %
Channel Quality Wait Time	120 sec
Minimum Scan Time	8
Load aware Scan Threshold	1250000 Bps
Mode Aware Arm	<input type="checkbox"/>
Scan Mode	all-reg-domain
Cellular handoff assist	<input type="checkbox"/>
Client Match	<input type="checkbox"/>

Apply

**8** Click **High-Throughput Radio Profile** (default-a).

**a** Check **Legacy Station** workaround.

**b** Click **Apply** and **Save Configuration**.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
AP  
Controller  
Campus WLAN  
Remote AP  
AirWave

NETWORK  
Controller  
VLANs  
Ports  
Cellular Profile  
IP

SECURITY  
Authentication  
Access Control

WIRELESS  
AP Configuration  
AP Installation

MANAGEMENT  
General  
Administration  
Certificates  
SNMP  
Logging  
Clock  
Guest Provisioning  
Captive Portal  
SMTP  
Bandwidth Calculator  
Threshold

ADVANCED SERVICES  
Redundancy  
AirGroup  
IP Mobility  
Stateful Firewall  
External Services  
VPN Services  
Wired Access  
All Profiles

**Configuration > AP Group > Edit "default"**

Profiles		Profile Details	
<input type="checkbox"/> Wireless LAN			
<input checked="" type="checkbox"/> Virtual AP			
<input type="checkbox"/> RF Management			
<input checked="" type="checkbox"/> 802.11a radio	default		
<input checked="" type="checkbox"/> Adaptive Radio Management (ARM)	default		
<input type="checkbox"/> High-throughput Radio	default-a		
<input type="checkbox"/> AM Scanning	default		
<input checked="" type="checkbox"/> 802.11g radio	default		
<input type="checkbox"/> RF Optimization	default		
<input type="checkbox"/> RF Event Thresholds	default		
<input checked="" type="checkbox"/> AP			
<input checked="" type="checkbox"/> QOS			
<input checked="" type="checkbox"/> IDS			
<input checked="" type="checkbox"/> Mesh			

Profile Details	
Basic	Advanced
Assignment	disable
Allowed bands for 40MHz channels	a-only
80MHz support	<input checked="" type="checkbox"/>
Client Aware	<input checked="" type="checkbox"/>
Max Tx EIRP	127
Min Tx EIRP	9
Rogue AP Aware	<input type="checkbox"/>
Active Scan	<input type="checkbox"/>
ARM Over the Air Updates	<input checked="" type="checkbox"/>
Scanning	<input checked="" type="checkbox"/>
Multi Band Scan	<input checked="" type="checkbox"/>
VoIP Aware Scan	<input checked="" type="checkbox"/>
Power Save Aware Scan	<input checked="" type="checkbox"/>
Video Aware Scan	<input checked="" type="checkbox"/>
Ideal Coverage Index	10
Acceptable Coverage Index	4
Free Channel Index	25
Backoff Time	240 sec
Error Rate Threshold	50 %
Error Rate Wait Time	30 sec
Channel Quality Aware Arm	<input type="checkbox"/>
Channel Quality Threshold	70 %
Channel Quality Wait Time	120 sec
Minimum Scan Time	8
Load aware Scan Threshold	1250000 Bps
Mode Aware Arm	<input type="checkbox"/>
Scan Mode	all-reg-domain
Cellular handoff assist	<input type="checkbox"/>
Client Match	<input type="checkbox"/>

Apply

## Assigning a 2.4 GHz Radio-profile

- 1 Click **802.11g radio-profile**.
- 2 Click the **Advanced** tab.
  - a Click **Radio enable** to turn the 802.11g radio on.
  - b In the default profile on the right-pane, enter a 2.4 GHz channel.
  - c Clear or set the High throughput enable (radio) according to whether the radio is 802.11n-enabled mode or not. Use only a 20 MHz width.
  - d Choose a Transmit EIRP chosen to support the site survey plan and the maximum mandatory data rate as described immediately below.



**Admin Tip: Transmit Power**

For setting up the **Transmit Power**, please consult your facility's RF site survey, designed for voice traffic, to determine if you have sufficient coverage to support all data rates. Spectralink Wireless Telephones require the following minimum dBm reading to support the corresponding **Mandatory** data rate setting in the access point.

<i>802.11 Radio Standard</i>	<i>Minimum Available Signal Strength (RSSI)</i>	<i>Maximum "Mandatory" Data Rate</i>
802.11b	-65 dBm	11 Mb/s
802.11g	-67 dBm	6 Mb/s
802.11g	-47 dBm	54 Mb/s

**Web Info: RF Deployment reference**

For additional details on RF deployment please see the *Deploying Enterprise-Grade Wi-Fi Telephony* White Paper.

Dashboard | Monitoring | **Configuration** | Diagnostics | Maintenance | Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave

NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP

SECURITY  
 Authentication  
 Access Control

WIRELESS  
 > **AP Configuration**  
 AP Installation

MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold

ADVANCED SERVICES  
 Redundancy  
 AirGroup  
 IP Mobility  
 Stateful Firewall  
 External Services  
 VPN Services  
 Wired Access  
 All Profiles

**Configuration > AP Group > Edit "default"**

Profiles		Profile Details	
<input type="checkbox"/> Wireless LAN		802.11g radio profile > default <span>Show Reference</span> <span>Save As</span> <span>Reset</span>	
<input type="checkbox"/> Virtual AP		Basic <span>Advanced</span>	
<input type="checkbox"/> RF Management		<b>General</b> Radio enable <input checked="" type="checkbox"/> Mode <span>ap-mode</span> High throughput enable (radio) <input checked="" type="checkbox"/> TurboQAM rates enable (radio) <input type="checkbox"/> Channel <span>6</span> <span>Channel Width: <input checked="" type="radio"/> 20MHz <input type="radio"/> 40MHz</span> Non-Wi-Fi Interference Immunity <span>2</span>	
<input type="checkbox"/> 802.11a radio	default		
Adaptive Radio Management (ARM)	default		
High-throughput Radio	default-a		
AM Scanning	default		
<input type="checkbox"/> 802.11g radio	default		
Adaptive Radio Management (ARM)	default		
High-throughput Radio	default-g		
AM Scanning	default		
RF Optimization	default		
RF Event Thresholds	default		
<input type="checkbox"/> AP			
<input type="checkbox"/> QOS			
<input type="checkbox"/> IDS			
<input type="checkbox"/> Mesh			

Apply

- 3 Click **Adaptive Radio Management (ARM) profile** and then the **Advanced** tab.
- 4 Enter the settings as follows
  - a Ensure that **Assignment** is set to **disable** or **maintain**.
  - b Set **Allowed bands for 40MHz channels** to **a-only**.
  - c Check **Client Aware**.
  - d Ensure that **Active Scan** is not checked.
  - e Ensure that **ARM Over the Air Updates, Scanning, Multi Band Scan, VoIP Aware Scan, Power Save Aware Scan, and Video Aware Scan** are checked.
  - f Ensure that **Client Match** is NOT checked.

Dashboard Monitoring **Configuration** Diagnostics Maintenance Save Configuration

WIZARDS  
 AP  
 Controller  
 Campus WLAN  
 Remote AP  
 AirWave  
 NETWORK  
 Controller  
 VLANs  
 Ports  
 Cellular Profile  
 IP  
 SECURITY  
 Authentication  
 Access Control  
 WIRELESS  
 > **AP Configuration**  
 AP Installation  
 MANAGEMENT  
 General  
 Administration  
 Certificates  
 SNMP  
 Logging  
 Clock  
 Guest Provisioning  
 Captive Portal  
 SMTP  
 Bandwidth Calculator  
 Threshold  
 ADVANCED SERVICES  
 Redundancy  
 AirGroup  
 IP Mobility  
 Stateful Firewall  
 External Services  
 VPN Services  
 Wired Access  
 All Profiles

**Configuration > AP Group > Edit "default"**

Profiles		Profile Details	
		Basic	Advanced
<input type="checkbox"/> Wireless LAN			
<input type="checkbox"/> Virtual AP			
<input type="checkbox"/> RF Management			
<input type="checkbox"/> 802.11a radio	default		
Adaptive Radio Management (ARM)	default		
High-throughput Radio	default-a		
AM Scanning	default		
<input type="checkbox"/> 802.11g radio	default		
Adaptive Radio Management (ARM)	default		
High-throughput Radio	default-g		
AM Scanning	default		
RF Optimization	default		
RF Event Thresholds	default		
<input type="checkbox"/> AP			
<input type="checkbox"/> QOS			
<input type="checkbox"/> IDS			
<input type="checkbox"/> Mesh			

Assignment: disable  
 Allowed bands for 40MHz channels: a-only  
 80MHz support: ☒  
 Client Aware: ☒  
 Max Tx EIRP: 127  
 Min Tx EIRP: 9  
 Rogue AP Aware: ☐  
 Active Scan: ☐  
 ARM Over the Air Updates: ☒  
 Scanning: ☒  
 Multi Band Scan: ☒  
 VoIP Aware Scan: ☒  
 Power Save Aware Scan: ☒  
 Video Aware Scan: ☒  
 Ideal Coverage Index: 10  
 Acceptable Coverage Index: 4  
 Free Channel Index: 25  
 Backoff Time: 240 sec  
 Error Rate Threshold: 50 %  
 Error Rate Wait Time: 30 sec  
 Channel Quality Aware Arm: ☐  
 Channel Quality Threshold: 70 %  
 Channel Quality Wait Time: 120 sec  
 Minimum Scan Time: 8  
 Load aware Scan Threshold: 1250000 Bps  
 Mode Aware Arm: ☐  
 Scan Mode: all-reg-domain  
 Cellular handoff assist: ☐  
 Client Match: ☐

Apply

**5** Click **High-Throughput Radio profile (default-g)** and then the **Advanced** tab.

**a** Check **CSD override**.

**b** Click **Apply**.

**6** Click **Save Configuration**.

At this point, the Mobility Controller is ready to provide Spectralink voice services.

\*\*\*\*END OF DOCUMENT\*\*\*\*